INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Interna ai Application No
PCT/US 00/21065

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5920822 A	06-07-1999	AU 717887 B	06-04-2000
		AU 1459397 A	11-08-1997
		BR 9707007 A	20-07-1999
		CA 2242334 A	24-07-1997
		CN 1214179 A	14-04-1999
		EP 0858713 A	19-08-1998
		WO 9726765 A	24-07-1997

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/19027 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US00/24623

(22) International Filing Date:
7 September 2000 (07.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
Not furnished 8 September 1999 (08.09.1999) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: ABROL, Nischal; 7260 Calle Cristobal, #41, San Diego, CA 92126 (US). LIOY, Marcello; 7588 Charmant Drive, #1924, San Diego, CA 92122 (US).

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

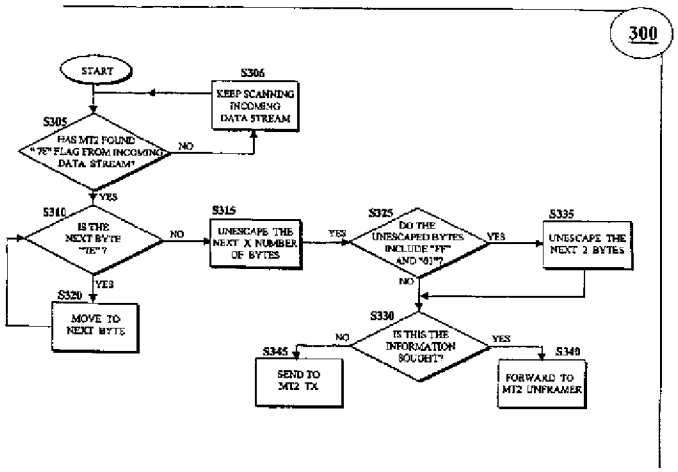
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: METHODS FOR EFFICIENT EARLY PROTOCOL DETECTION



(57) Abstract: A method and system that detects protocol and configuration messages in a PPP packet without having to unframe the entire packet. The method includes a communication device (MT2) that receives a plurality data frames (S306), wherein the communication device is capable of ascertaining the beginning of an information portion (S305) within the received frames. The communications device detects whether the information portion contains configuration information, such as protocol and configuration messages of a predetermined type. In a first embodiment, the detection is achieved by the communication device unescaping (S315) the contents of a plurality of bytes and determining (S325, S330, S335) whether the escaped bytes contains the desired configuration information. In a second embodiment, the communication device determines whether the contents of a particular byte contain the desired configuration information, in escaped or unescaped form, and the communication device continues to sequentially process the bytes within the information portion until the bytes typically containing the desired configuration information are processed.

WO 01/19027 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHODS FOR EFFICIENT EARLY PROTOCOL DETECTION

BACKGROUND OF THE INVENTION

I. Field of the Invention

This invention generally relates to the field of wireless communications. More particularly, the present invention relates to a novel method and system for performing early protocol and configuration message detection without having to unframe entire PPP packets.

II. Description of Related Art

Recent innovations in wireless communication and computer-related technologies, as well as the unprecedented growth of Internet subscribers, have paved the way for mobile computing. In fact, the popularity of mobile computing has placed greater demands on the current Internet infrastructure to provide mobile users with more support. A crucial part of meeting these demands and providing users with the necessary support is the use of Code Division Multiple Access (CDMA) technology in wireless communication systems.

CDMA is a digital radio-frequency (RF) channelization technique defined in the Telecommunications Industry Association/Electronics Industries Association Interim Standard-95 (TIA/EIA IS-95), entitled "MOBILE STATION-BASE STATION COMPATIBILITY STANDARD FOR DUAL-MODE WIDEBAND SPREAD SPECTRUM CELLULAR SYSTEM", published in July 1993 and herein incorporated by reference. Wireless communication systems employing this technology assign a unique code to communication signals and spread these communication signals across a common (wideband) spread spectrum bandwidth. As long as the receiving apparatus in a CDMA system has the correct code, it can successfully detect and select its communication signal from the other signals concurrently transmitted over the same frequency band. The use of CDMA produces an increase in system

traffic capacity, improves overall call quality and noise reduction, and provides a reliable transport mechanism for data service traffic.

FIG. 1 illustrates the basic elements of such a wireless data communication system **100**. Artisans of ordinary skill will readily appreciate that these elements, or their interfaces, may be modified, augmented, or subjected to various standards known in the art, without limiting their scope or function. System **100** allows a mobile terminal equipment, TE2 device **102** (e.g., the terminal equipment such as laptop or palmtop computer) to communicate with an Interworking Function (IWF) **108**. System **100** includes a wireless communication device, MT2 device **104** (e.g., wireless telephone), and a Base Station/Mobile Switching Center (BS/MSC) **106**. The IWF **108** serves as a gateway between the wireless network and other networks, such as the Public Switched Telephone Network or wireline packet data networks providing Internet- or Intranet-based access.

As shown in FIG. 1, the IWF **108** is coupled to the BS/MSC **106**, via the L interface. Often the IWF **108** will be co-located with the BS/MSC **106**. The TE2 device **102** is electronically coupled to the MT2 device **104** via the R_m interface. The MT2 device **104** communicates with the BS/MSC **106** via the wireless interface U_m. The TE2 device **102** and the MT2 device **104** may be integrated into a single unit or may be separated out, as in the case of an installed mobile phone unit in which a laptop is the TE2 device **102** and the transceiver is the MT2 device **104**. It is important to note that, as indicated by FIG. 2, the combination of the TE2 device **102** and the MT2 device **104**, whether integrated or separate, is generally referred to as a mobile station (MS) **103**.

Other support is made possible by applying various well-known protocols to control, manage, or otherwise facilitate different aspects of wireless communications. For example, the life-blood of the Internet infrastructure, the Internet Protocol (IP), has been incorporated in wireless communications to accommodate packet-oriented services. The IP protocol specifies the addressing and routing of packets (datagrams) between host computers and is defined in Request For Comment 791 (RFC 791) entitled, "INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL

SPECIFICATION," published September 1981, and herein incorporated by reference.

The IP protocol is a network layer protocol that encapsulates data into IP packets for transmission. Addressing information is affixed to the header of the packet. IP headers (e.g., IP version 4) contain 32-bit addresses that identify the sending and receiving hosts. These addresses are used by intermediate routers to select a path through the network for the packet towards its ultimate destination at the intended address. Thus, the IP protocol allows packets originating at any Internet node in the world to be routed to any other Internet node in the world, given that the originating party knows the IP address of the destination party.

Another well-known protocol which has been incorporated in wireless communications systems is the Point-to-Point Protocol (PPP) protocol, which provides, *inter alia*, Internet access. The PPP protocol is described in detail in Request for Comments 1661 (RFC 1661), entitled "THE POINT-TO-POINT PROTOCOL (PPP)", published July 1994 and herein incorporated by reference.

Essentially, the PPP protocol specifies a method for transporting multi-protocol datagrams over point-to-point links and contains three main components: a method of encapsulating multi-protocol datagrams over serial links; a Link Control Protocol (LCP) for establishing, testing, configuring, and maintaining a data link connection; and a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

In an effort to provide a host of services on wireless communication systems, various standards have been developed to accommodate the wireless data transmission between the TE2 device **102** and the IWF **108**. For example, the TIA/EIA IS-707.5 standard, entitled "DATA SERVICE OPTIONS FOR WIDEBAND SPREAD SPECTRUM SYSTEMS: PACKET DATA SERVICES," published February 1998, and herein incorporated by reference, defines requirements for support of packet data transmission capability on TIA/EIA IS-95 systems and specifies a suite of packet data bearer services. Similarly, the TIA/EIA IS-707-A.5 standard, entitled "DATA

SERVICE OPTIONS FOR SPREAD SPECTRUM SYSTEMS: PACKET DATA SERVICES," and the TIA/EIA IS-707-A.9 standard, entitled "DATA SERVICE OPTIONS FOR SPREAD SPECTRUM SYSTEMS: HIGH-SPEED PACKET DATA SERVICES," both published in March 1999 and incorporated by reference, also define requirements for packet data transmission support on TIA/EIA IS-95 systems.

These standards provide that certain packet data service options that may be used to communicate between the TE2 device **102** and IWF **108** via BS/MSC **106**. In doing so, IS-707.5 introduces the Network Model, which details the packet data protocol requirements for the R_m interface, U_m interface, and the L interface. Under this model, two separate PPP links are provided at the data link layer: a first PPP link (PPP_R) provides the data link layer between the TE2 device **102** and the MT2 device **104** (i.e., across the R_m interface), and a second PPP link (PPP_U), independent of the first, provides the data link layer between the MT2 device **104** and the IWF **108** (i.e., across the U_m and L interfaces).

The separate and independent PPP links help support "transparent mobility"; that is, the TE2 device **102** should experience seamless and transparent service, regardless of time and its current IWF **108** point-of-attachment. As such, the TE2 device **102** should not be affected by location changes. For example, the TE2 device **102** should not be affected from PPP renegotiations occurring on the U_m link, such as when MT2 device **104** attempts to attach to a different IWF **108**. Thus, the Network Model operates to isolate the PPP_R link from the PPP_U link in order to prevent changes on the U_m link from affecting the R_m link. In other words, the PPP_U link can be renegotiated without forcing the PPP_R link to be renegotiated.

FIG. 2 illustrates the protocol stacks in each entity of the IS-707.5 Network Model. At the far left of FIG. 2 is a protocol stack, shown in conventional vertical format, depicting the protocol layers running on the TE2 device **102** (e.g., the mobile terminal, laptop or palmtop computer). The TE2 device **104** protocol stack is illustrated as being logically connected to the MT2 device **104** protocol stack over the R_m interface. The MT2 device **104**, is illustrated as being logically connected to the BS/MSC **106** protocol stack

over the U_m interface. The BS/MSC **106** protocol stack is, in turn, shown as being logically connected to the IWF **108** protocol stack over the L interface.

By way of example, the protocols depicted in FIG. 2, operate as follows: the PPP_R protocol **208** on the TE2 **102** device encodes packets from the upper layer protocols **204**, and the network layer IP protocol **206**. The PPP_R protocol **208** then transmits the packets across the R_m interface using the TIA/EIA 232-F protocol **210** to the TIA/EIA-232-F-compatible port on the MT2 device **104** running the TIA/EIA 232-F protocol **212**. The TIA/EIA-232-F standard is defined in "INTERFACE BETWEEN DATA TERMINAL EQUIPMENT AND DATA CIRCUIT-TERMINATING EQUIPMENT EMPLOYING SERIAL BINARY DATA INTERCHANGE", published in October 1997 and herein incorporated by reference. It is to be understood that other standards or protocols known to artisans of ordinary skill in the art may be used to define the transmission across the R_m interface. For example, other applicable R_m interface standards include, the "UNIVERSAL SERIAL BUS (USB) SPECIFICATION, Revision 1.1", published in September 1998, and the "BLUETOOTH SPECIFICATION VERSION 1.0A CORE, published in July 1999, both incorporated by reference.

The TIA/EIA 232-F protocol **212** on the MT2 device **104** receives the packets from the TE2 device **102** and passes them to the PPP_R protocol **213**. As stated above, the PPP_R protocol **213** unframes the packets encapsulated in the PPP frames and typically, when a data connection is up, the protocol **213** transfers the packets to PPP_U protocol **217**. Protocol **217** essentially re-frames the packets for transmission to a PPP_U peer located in the IWF **108**. The Radio Link Protocol (RLP) **216** and IS-95 protocol **214**, both of which are well known in the art, are used to transmit the packet-encapsulated PPP frames to the BS/MSC **106** over the U_m interface. The RLP protocol **216** is defined in the IS-707.2 standard, entitled "DATA SERVICE OPTIONS FOR WIDEBAND SPREAD SPECTRUM SYSTEMS: RADIO LINK PROTOCOL", published in February 1998 and herein incorporated by reference, as well as the IS-707-A.2 standard, entitled "DATA SERVICE OPTIONS FOR SPREAD SPECTRUM SYSTEMS: RADIO LINK PROTOCOL", published in March 1999 and also incorporated by reference.

A corresponding RLP protocol **220** and IS-95 protocol **222** in the BS/MSC **106** transfer the packets to the relay layer protocol **224** for transmission across the L interface to the relay layer protocol **224** on the IWF **108**. The PPP_U protocol **232** then unframes the received packets and transfers them to the network layer protocol IP **230**, which in turn passes them to the upper layer protocols **228** or forwards them to the Internet.

As stated above, the PPP_R protocol **213** transfers the packets to the PPP_U protocol **217** when a data link connection is established. RFC 1661 provides that Link Control Protocol (LCP) packets must be exchanged and negotiated over each PPP link (i.e., PPP_R and PPP_U) in order to establish, configure, and test the data link connection. As such, these LCP packets comprise Configure-Request, Configure-Ack, Configure-Nak, Protocol-Reject, and Configure-Reject messages to negotiate various options and operate as follows: the Configure-Request packet is used to negotiate configuration options. The Configuration-Ack packet is only transmitted if every configuration option in a received Configuration-Request packet is recognizable and all values are acceptable. The Configure-Nak packet is sent when the requested configuration options in a Configuration-Request packet are recognizable but contain values that are not acceptable and the Configure-Nak Options field is filled with the unacceptable Configure-Request configuration options and suggested values that will work. The Configure-Reject packet is sent when the requested configuration options in a Configure-Request includes configuration options that are not understood by the receiver and the Configure-Reject Options field contains the unrecognized Configure-Request configuration options.

Once the LCP packets are exchanged, the link options negotiated, and the data link connection established, a network layer connection must be established between the TE2 device **102** and the IWF **108**. Such a connection is achieved through protocols **206, 212, 218, 230**, which include, for example, the IP protocol. The negotiating, configuring, enabling, and disabling of the IP protocol on both ends of the PPP links is provided by the Internet Protocol Control Protocol (IPCP). IPCP is a part of a family of Network Control Protocols (NCPs) included in the PPP protocol and is described in Request for

Comment (RFC) 1332, "THE PPP INTERNET PROTOCOL CONTROL PROTOCOL (IPCP)", published in May 1992 and herein incorporated by reference.

The IPCP protocol uses the same configuration option negotiation mechanism as the LCP protocol and, much like the LCP protocol, IPCP negotiations occur separately for both the R_m interface and the U_m interface. As described in RFC 1661, the Configuration-Ack packet contains a list of the options, which the Sender is acknowledging. The MT2 device **104** monitors the received and transmitted Configuration-Ack packets over the R_m and U_m interfaces and stores the value of each option in a storage device, such as a computer memory. All configuration options have default values, defined by RFC 1661, which are used when the corresponding configuration option is not negotiated. It is to be noted that the configuration option default values may be defined by other RFCs, such as, for example, RFC 1877 entitled "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses" published in December 1995 and incorporated by reference.

As stated above with respect to the Network Model, the PPP_U link can be renegotiated without forcing the PPP_R link to be renegotiated. To maintain such isolation between the R_m and U_m interfaces, the MT2 device **104** generally unframes and reframes received PPP packets. Unless packets received by the MT2 device **104** are to be passed to an executing upper layer protocol within the MT2 device **104**, the PPP packets are unframed only to be reframed for subsequent transmission to a PPP peer protocol. This unframing/reframing occurs even when the packets require no further processing in the MT2 device **104**. For example, when a call is initially brought up, the LCP and IPCP mechanisms can negotiate to establish identical configuration options for both the U_m and R_m interfaces. As long as the configuration options remain identical, all of the PPP data packets (as opposed to the configuration packets) could "pass through", from one interface to the other, without the MT2 device **104** unframing/reframing the packets. Clearly, in cases where the configuration options remain identical, the MT2 device **104** performs too many unnecessary PPP packet

unframing/reframing operations. Such operations adversely affect the processing resources and throughput latency of the MT2 device **104**.

However, if the configuration options change, they must be renegotiated, which militates in favor of unframing/reframing the PPP packets. For example, by virtue of the fact that the MT2 device **104** is mobile, it is capable of moving to an area that is served by an IWF **108** that is different from the original IWF **108**. When this happens, the MT2 device **104** will be "handed off" to the new IWF **108** for service. This handoff requires the renegotiation of particular LCP and IPCP configuration options over the U_m interface as well as the intervention of the MT2 device **104**. If the packets containing the configuration option messages (e.g., Configure-Request, Configure-Ack, Configure-Nak, etc.) were simply "passed through", without unframing or examining the contents of the packets, the packets would force the end-to-end resynchronization of the entire link which would terminate the independence of the R_m and U_m links.

Therefore, what is needed is a novel and efficient method and system capable of early protocol and configuration message detection without having to unframe a PPP packet.

SUMMARY OF THE INVENTION

The present invention addresses the need identified above by providing a method and system that detects protocol and configuration messages in a PPP packet without having to unframe the entire packet.

Methods and systems consistent with the principles of the present invention as embodied and broadly described herein include a communication device that receives a plurality data frames, wherein the communication device is capable of ascertaining the beginning of an information portion within the received frames. The communications device detects whether the information portion contains configuration information, such as protocol and configuration messages of a predetermined type. In a first embodiment, the detection is achieved by the communication device unescaping the contents of a plurality of bytes and

determining whether the escaped bytes contains the desired configuration information. In a second embodiment, the communication device determines whether the contents of a particular byte contain the desired configuration information, in escaped or unescaped form, and the communication device continues to sequentially process the bytes within the information portion until the bytes typically containing the desired configuration information are processed or it is determined that the information does not exist.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this Specification, illustrate an embodiment of the invention and, together with the description, explain the objects, advantages, and principles of the invention. In the drawings:

FIG. 1 is a high level block diagram depicting various elements of a wireless communication system.

FIG. 2 schematically describes the protocol stacks of a wireless communication system.

FIG. 3 is a flow-chart diagrams describing a first embodiment of the invention.

FIGS. 4A, 4B are flow-chart diagrams describing a second embodiment of the invention.

FIG. 5 describes the general format of a packet encapsulated in a PPP frame.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following detailed description of the embodiments of the present invention refers to the accompanying drawings that illustrate these. Other embodiments are possible and modifications may be made to the embodiments without departing from the spirit and scope of the invention.

Therefore, the following detailed description is not meant to limit the invention. Rather the scope of the invention is defined by the appended claims.

It will be apparent to one of ordinary skill in the art that an embodiment of the present invention, as described below, may be realized in a variety of implementations, including the software, firmware, and hardware of the entities illustrated in the figures (i.e., TE2 device **102**, MT2 device **104**, BS/MSC **106** and IWF **108**). The actual software code or control hardware used to implement the present invention is not limiting of the present invention. Thus, the operation and behavior of the present invention will be described without specific reference to the actual software code or hardware components. Such non-specific references are acceptable because it is clearly understood that a person of ordinary skill in the art would be able to design software and control hardware to implement the embodiment of the present invention based on the description herein.

Because the embodiments described herein operate on PPP packets encapsulated in HDLC frames, FIG. 5 illustrates the various attributes of such packets. The beginning (and end) of the frame is demarcated by a 1-byte framing flag represented by the hexadecimal character "7E". The following two bytes indicate the protocol address and control field which, for standard PPP packets, are typically designated as the hexadecimal characters "FF" and "03", respectively. The next two bytes indicate the protocol type, such as, for example, the LCP protocol, denoted by the hexadecimal characters "C0" and "21"; the IPCP protocol, indicated by the hexadecimal characters "80" and "21"; or the Van Jacobson protocol compressed state, indicated by the hexadecimal characters "00" (which may be compressed out) and "2D". The subsequent byte indicates the code or the configuration message, such as Configure-Request, denoted by the hexadecimal character "01"; Configure-Ack, indicated by the hexadecimal character "02"; or Configure-Nak, indicated by the hexadecimal character "03".

1. **First Embodiment**

FIG. 3 is a flow-chart diagram depicting a first embodiment of the present invention. As such, FIG. 3 details the operation of the MT2 device **104** for performing early protocol and configuration message detection in PPP packets.

In step **S305**, the MT2 device **104**, first scans an incoming data stream to detect the framing flag, indicated by the hexadecimal character "7E". This flag demarcates a frame and can, therefore, be used to indicate the beginning and/or end of packets encapsulated in PPP frames. If the MT2 device **104** has not detected a "7E" framing flag, it keeps scanning the incoming data, as indicated by step **S306**, until it detects the flag. Once the MT2 device **104** detects the "7E" framing flag, it progresses to step **S310**.

After detecting a "7E" flag, the MT2 device **104**, in step **S310**, determines whether the next byte is also a "7E" flag. If so, the MT2 device **104** skips that particular byte, as indicated in step **S320**, and returns back to step **S310** to apply the "7E" flag test to the next byte. If the next byte is not a "7E" flag, the MT2 device **104** progresses to step **S315**. It is important to note that the incoming data stream may contain consecutive "7E" flags, as in the case of back-to-back packets where a "7E" flag, indicating the end of a frame, is juxtaposed to a subsequent "7E" flag, indicating the beginning of a new frame. Steps **S310** and **S320** operate to filter out the framing flags, enabling the MT2 device **104** to discern where the information portion of the framed packet begins.

Aware that the next byte is not a "7E" flag, but an information byte, the MT2 device **104** in step **S315**, "unescapes" the next X number of bytes, where X corresponds to the relative position of the information sought within the framed-packet. This unescaping is performed because, as is well known in the art, when the PPP protocol is transmitted with asynchronous, HDLC-like framing (i.e., as per RFC 1662), the protocol employs an "escaping technique" to mask certain characters within the information portion of a packet that also function as special control characters. Such characters include the aforementioned "7E" flag as well as the escape flag "7D". When these characters are encountered in the information portion of a framed-

packet, the escaping technique stuffs the escape flag "7D" in front of the character and modifies the character in order to neutralize its control function. Therefore, in seeking to detect certain protocol or configuration information from an incoming data stream, the MT2 device **104**, in step **S315**, unescapes the number of bytes necessary to access the information sought in order to uncover its true identity. After unescaping X bytes, the MT2 device **104** proceeds to step **S325**.

In step **S325**, the MT2 device **104** determines whether the unescaped X bytes include the standard PPP address and control field characters "FF" and "03", respectively. Although these characters typically comprise the first and second bytes of the information portion of a PPP packet (*see, e.g.,* FIG. 5), these characters may be compressed out of the packet, thereby affecting the location of the ensuing information bytes. Therefore, the MT2 device **104** must check whether these characters are included within the unescaped bytes of the packet in order to make the necessary adjustments later. If the characters "FF" and "03" are not included in the unescaped bytes (i.e., characters "FF" and "03" are compressed out), the MT2 device **104**, in step **S330**, checks to see whether these bytes contain the protocol or configuration message information being sought. If they do, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer, in order to unframe the packet and engage in the processing indicated by the detected information. If the bytes do not contain the information being sought, the MT2 device **104** sends the entire packet to the MT2 device **104** transmit portion to be forwarded across the pertinent interface, as indicated by step **S345**.

Returning to step **S325**, if the unescaped X bytes include "FF" and "03", the MT2 device **104**, in step **S335**, compensates by unescaping another 2 bytes, in addition to the specified X bytes. This adjusts for the inclusion of the "FF" and "03" characters within the X bytes. The MT2 device **104** then submits the X + 2 unescaped bytes to step **S330**, where, as stated above, it checks to see whether the unescaped bytes contain the desired information. If they do, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer. If the bytes do not contain the protocol or

configuration message information being sought, the MT2 device **104**, in step **S345**, sends the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface.

To illustrate the operation of this embodiment, suppose the early detection of an LCP protocol packet is desired. The LCP protocol specification is provided within the protocol information portion of a PPP-framed packet. As indicated in FIG. 5, the protocol information is 2 bytes long, typically occupying byte positions 3 and 4 of the information portion of a standard PPP-framed packet. After scanning the incoming data stream and discerning where the information bytes begin (i.e., steps **S305**, **S310**, and **S320**), the MT2 device **104** unescapes the next two bytes (i.e., X equal to 2), as indicated by step **S315**. If, in step **S325**, the first 2 bytes do not include the "FF" and "03" characters, then the MT2 device **104** checks to see whether these bytes contain the LCP information being sought. If it does, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer, in order to unframe the packet and engage in the processing required by the LCP protocol information. If the bytes do not contain the LCP information, the MT2 device **104** sends the entire packet to the MT2 device **104** transmit portion to be forwarded across the pertinent interface, as indicated by step **S345**.

If, on the other hand, the first two bytes of the unescaped X bytes are "FF" and "03", the MT2 device **104**, in step **S335**, compensates by unescaping the next 2 bytes, in addition to the first two bytes. The MT2 device **104** then submits all four unescaped bytes to step **S330**, where, as stated above, it checks to see whether these bytes contain the LCP information being sought. If they do, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer. If the bytes do not contain the LCP information, the MT2 device **104**, in step **S345**, sends the entire packet to the MT2 device **104** transmit portion.

It is important to note that, by virtue of the embodiment described above, all of the header information contained within the PPP-framed packet can be detected without unframing the entire packet. For example, by simply adjusting the X value in step **S315**, this embodiment can detect such

PPP information as protocol information, configuration messages, packet ID, etc.

Thus, this embodiment detects protocol and configuration messages within a PPP packet stream without having to unframe the entire packets. Rather, by unescaping certain bytes within the information portion of the packets, this embodiment provides a system and method that efficiently detects protocol and configuration messages without performing unnecessary PPP packet unframing/reframing operations.

2. **Second Embodiment**

FIGS. 4A, 4B are flow-chart diagrams depicting a second embodiment of the present invention. This embodiment detects protocol and configuration messages contained within the information portion of a PPP-framed packet by scanning the incoming data stream and mechanically checking the information bytes in stages, without unframing the packets. Given the format of the PPP-framed packets, as illustrated by FIG. 5, the first stage specifically detects the content of the 1-byte address field, contained within the information portion of the packet. The second stage is directed to detecting the contents of the 1-byte control field, which follows the address field. Accordingly, this embodiment is capable of advancing the stages, and detecting the contents of all information fields, until the end of the information portion. For example, a third stage could be directed to detecting the contents of the 2-byte protocol field, which follow the control field. However, because of the PPP-framed packet structure and the sequential nature of this embodiment, information contained in the later fields of the frame, is generally detected after processing and detecting information contained in the preceding fields.

As a representative example of this embodiment, suppose the information sought is contained within the control field. To access this field and detect the pertinent information from an incoming data stream, the MT2 device **104** must first identify the beginning of the information portion of the PPP packet and then access and detect the information in the address

field. Only after processing the address field information, is the MT2 device **104** ready to access and detect the control field information.

As such, FIG. 4A illustrates the first stage of this embodiment. In step **S405**, the MT2 device **104** first scans the incoming data stream to detect the framing flag "7E". After detecting the "7E" flag, the MT2 device **104**, in step **S410**, determines whether the next byte is also a "7E" flag. If it is, the MT2 device **104** moves to the next byte, as indicated in step **S415**, and returns back to step **S410** to apply the "7E" flag test to the next byte. If the next byte is not a "7E" flag, the MT2 device **104** progresses to step **S420**. As stated above with respect to the first embodiment, steps **S410** and **S415** operate to filter out the framing flags, allowing the MT2 device **104** to identify the beginning of the information portion of the PPP-framed packet.

Once the MT2 device **104** is able to identify the beginning information portion, it exploits the format of PPP packets to detect the information in stages. As stated above, the first stage of this embodiment is to detect the character "FF".

In step **S420**, the MT2 device **104** checks to see whether the first information byte is the escape character "7D". As indicated above, the escaping technique stuffs the escape flag "7D" in front of certain characters and masks them. If the first information byte is not "7D" (i.e., the first information byte is not escaped), the MT2 device **104**, in step **S425**, checks to see if the first information byte is the "FF" character (i.e., in unescaped form). If it is, the MT2 device **104** proceeds to step **S435**. If first information byte is not the "FF" character, the MT2 device **104** determines, in step **S426**, whether there is more information within the framed-packet to be sought, and if there is, the MT2 device **104** moves onto the next stage in step **S427**. If there is no additional desired information, the MT2 device **104**, in step **S428**, sends the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface.

Returning to step **S420**, if the first information byte is "7D" (i.e., the first information byte is escaped), the MT2 device **104**, in step **S430**, checks to see whether the next byte is the "FF" character in the escaped format (i.e., hexadecimal character "DF"). If it is, the MT2 device **104** proceeds to step

S435. If the next byte is not the "DF" character, the MT2 device **104** proceeds to step **S426** where, as stated above, the MT2 device **104** checks to see whether there is more desired information. If there is, the MT2 device **104** moves onto the next stage in step **S427**. If there is no additional desired information, the MT2 device **104**, in step **S428**, sends the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface.

If, in step **S430**, the next byte is the "FF" character in the escaped format (i.e., hexadecimal character "DF"), the MT2 device **104** proceeds to step **S435**, where it checks to see whether there is more information to be sought. If there is, the MT2 device **104** moves onto the next stage in step **S427**. If there is no additional desired information, the MT2 device **104**, in step **S437**, forwards the entire packet to the MT2 device **104** unframer, in order to unframe the packet and engage in the processing indicated by the detected information.

After completing the first stage of the embodiment (i.e., the detection of the "FF" character in the protocol address field), the MT2 device **104** must, consistent with the object of the representative example, endeavor to detect the "03" character in the control field. As noted above, this detection is referred to as the second stage detection for this embodiment and is depicted in FIG. 4B.

Upon completing the first stage, as indicated by step **S427**, the MT2 device **104**, in step **S440**, determines, once again, whether the next byte is the "7D" character. As stated above, this determination is used in case the characters within the relevant information field were escaped. If the next byte is not the "7D" character, the MT2 device **104**, in step **S445**, determines whether the byte is the "03" character (i.e., in unescaped format). If it is, the MT2 device **104** progresses to step **S435** where, as previously noted, the MT2 device **104** determines whether there is additional information being sought, and if there is the MT2 device **104** moves onto the next stage, as per step **S427**. Otherwise, the MT2 device **104**, in step **S428**, forwards the entire packet to the MT2 device **104** transmit portion to forward the packet across the relevant interface.

Returning to step **S440**, if the MT2 device **104** determines that the following byte is the "7D" character, it checks to see, in step **S450**, whether the subsequent byte is the "03" character in the escaped format (i.e., hexadecimal character "23"). If the subsequent byte is not the "23" character, the MT2 device **104** proceeds to step **S426**, to determine whether to move onto the next stage, as in step **S427**, or send the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface, as in step **S428**. If the subsequent byte is the "23" character, the MT2 device **104** proceeds to step **S435** where it determines whether to move onto the next stage, as in step **S427**, or forward the entire packet to the MT2 device **104** unframer, as in step **S437**.

Thus, this embodiment detects protocol and configuration messages within a PPP packet stream without having to unframe the packets. Rather, this embodiment scans the incoming data stream and mechanically checks the information bytes in stages. These stages correspond to the information fields of the PPP-framed packets and, therefore, this embodiment detects the desired information sequentially without performing unnecessary PPP packet unframing/reframing operations and without ignoring messages affecting link configurations.

The foregoing description of preferred embodiments of the present invention provides illustration and description, but is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible consistent with the above teachings or may be acquired from practice of the invention. Accordingly, the scope of the invention is defined by the claims and their equivalents.

What is claimed is:

CLAIMS

1. A method for early detection of configuration information of a predetermined type, said method comprising:

receiving, on a communication device, a plurality of framed data packets, each of said framed data packets containing an information portion;

detecting, on said communication device, a beginning of said information portion within one of said framed data packets; and

determining, on said communication device, whether said information portion contains said configuration information of a predetermined type,

wherein said communication device unframes said one of said framed data packets when said information portion contains said configuration information of a predetermined type.

2. The method of Claim 1, wherein said detecting includes scanning said plurality of said framed data packets and establishing said beginning of said information portion for one of said framed data packets by identifying a frame-demarcating character.

3. The method of Claim 2, wherein said detecting includes,

unescaping, on said communication device, contents of a predetermined number of bytes within said information portion, and

determining, on said communication device, whether said contents of said unescaped predetermined number of bytes includes predetermined characters,

wherein said communication device unescapes contents of additional consecutive bytes, succeeding said predetermined number of bytes, when said contents of said unescaped predetermined number of bytes includes said predetermined characters, and

wherein said communication device determines whether contents of said unescaped predetermined number of bytes and contents of additional

consecutive bytes contain said configuration information of a predetermined type.

4. The method of Claim 2, wherein said detecting includes,

determining, on said communication device, whether contents of a particular byte or bytes of said information portion contains information of a type associated with said particular byte, and

determining, on said communication device, whether said contents of said particular byte contains said configuration information of a predetermined type,

wherein said communication device progresses to a subsequent stage when said contents of said particular byte lacks said configuration information of a predetermined type and said configuration information of a predetermined type is disposed in a byte position subsequent to said particular byte.

5. The method of Claim 4, wherein said progresses to a subsequent stage further includes,

examining, on said communications device, contents of at least one succeeding byte of said information portion, said succeeding byte being subsequent to said particular byte, and

determining, on said communication device, whether contents of said succeeding byte contains information of a type associated with said succeeding byte, and

determining, on said communication device, whether said contents of said succeeding byte contains said configuration information of a predetermined type,

wherein said communication device sequentially examines successive bytes of said information portion until contents of said succeeding byte contains said configuration information of a predetermined type.

6. The method of Claim 5, wherein said contents of said particular byte and said contents of said succeeding byte includes escaped information.

7. The method of Claim 5, wherein said contents of said particular byte and said contents of said succeeding byte includes unescaped information.

8. A system for early detection of configuration information of a predetermined type, said system comprising:

a terminal device for transmitting and receiving a plurality of framed data packets, each of said framed data packets containing an information portion; and

a communication device coupled to said terminal device,

wherein said communication device detects a beginning of said information portion within one of said framed data packets and determines whether said information portion contains said configuration information of a predetermined type, and

wherein said communication device unframes said one of said framed data packets when said information portion contains said configuration information of a predetermined type.

9. The system of Claim 8, wherein said detecting by said communication device includes scanning said plurality of said framed data packets and establishing said beginning of said information portion for one of said framed data packets by identifying a frame-demarcating character.

10. The system of Claim 9, wherein said detecting by said communication device includes,

unescaping contents of a predetermined number of bytes within said information portion, and

determining whether said contents of said unescaped predetermined number of bytes includes predetermined characters,

wherein said communication device unescapes contents of additional consecutive bytes, succeeding said predetermined number of bytes, when said contents of said unescaped predetermined number of bytes includes said predetermined characters, and

wherein said communication device determines whether contents of said unescaped predetermined number of bytes and contents of additional consecutive bytes contain said configuration information of a predetermined type.

11. The system of Claim 9, wherein said detecting by said communication device includes,

determining whether contents of a particular byte or bytes of said information portion contains information of a type associated with said particular byte or bytes, and

determining whether said contents of said particular byte or bytes contains said configuration information of a predetermined type,

wherein said communication device progresses to a subsequent stage when said contents of said particular byte or bytes lacks said configuration information of a predetermined type and said configuration information of a predetermined type is disposed in a byte position subsequent to said particular byte or bytes.

12. The system of Claim 11, wherein said communication device progressing to a subsequent stage further includes,

examining contents of at least one succeeding byte of said information portion, said succeeding byte being subsequent to said particular byte, and

determining whether contents of said succeeding byte contains information of a type associated with said succeeding byte and whether said contents of said succeeding byte contains said configuration information of a predetermined type,

wherein said communication device sequentially examines successive bytes of said information portion until contents of said

succeeding byte contains said configuration information of a predetermined type.

13. The method of Claim 12, wherein said contents of said particular byte and said contents of said succeeding byte includes escaped information.

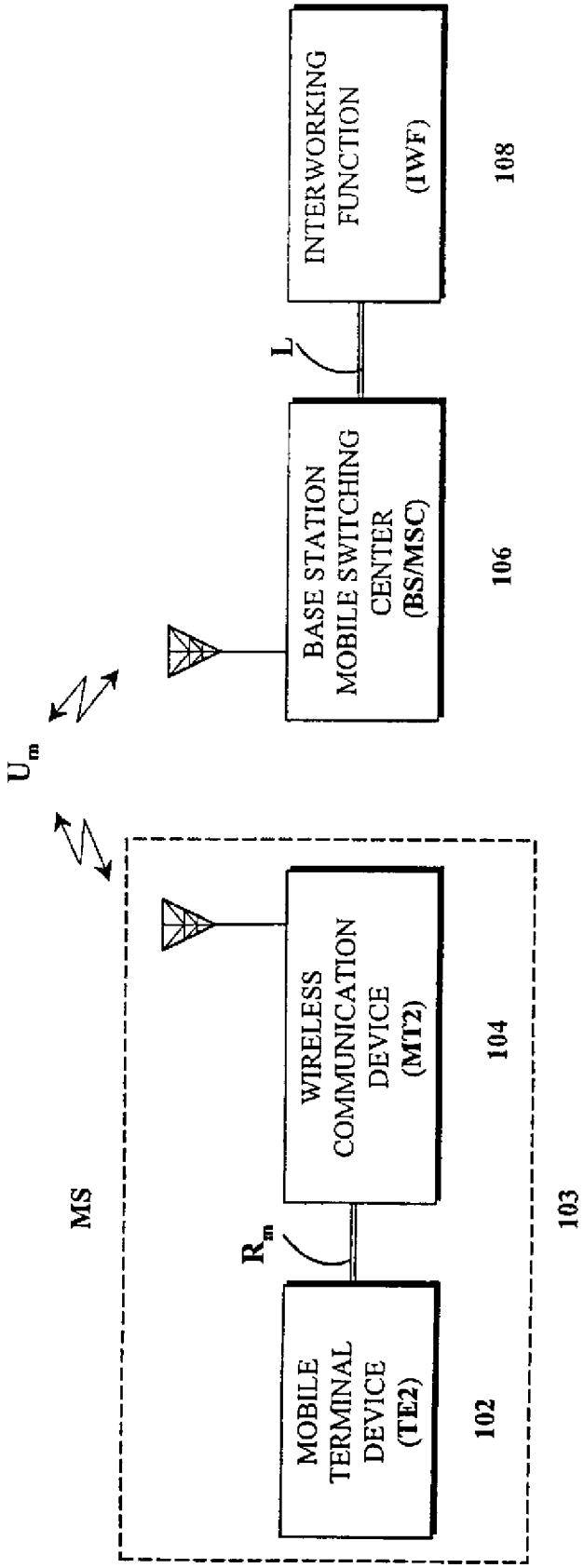

INTERWORKING FUNCTION (IWF)
108
L
BASE STATION MOBILE SWITCHING CENTER (BS/MSC)
106
U_m
WIRELESS COMMUNICATION DEVICE (MT2)
104
MS
R_m
MOBILE TERMINAL DEVICE (TE2)
102
103
100

FIG. 1

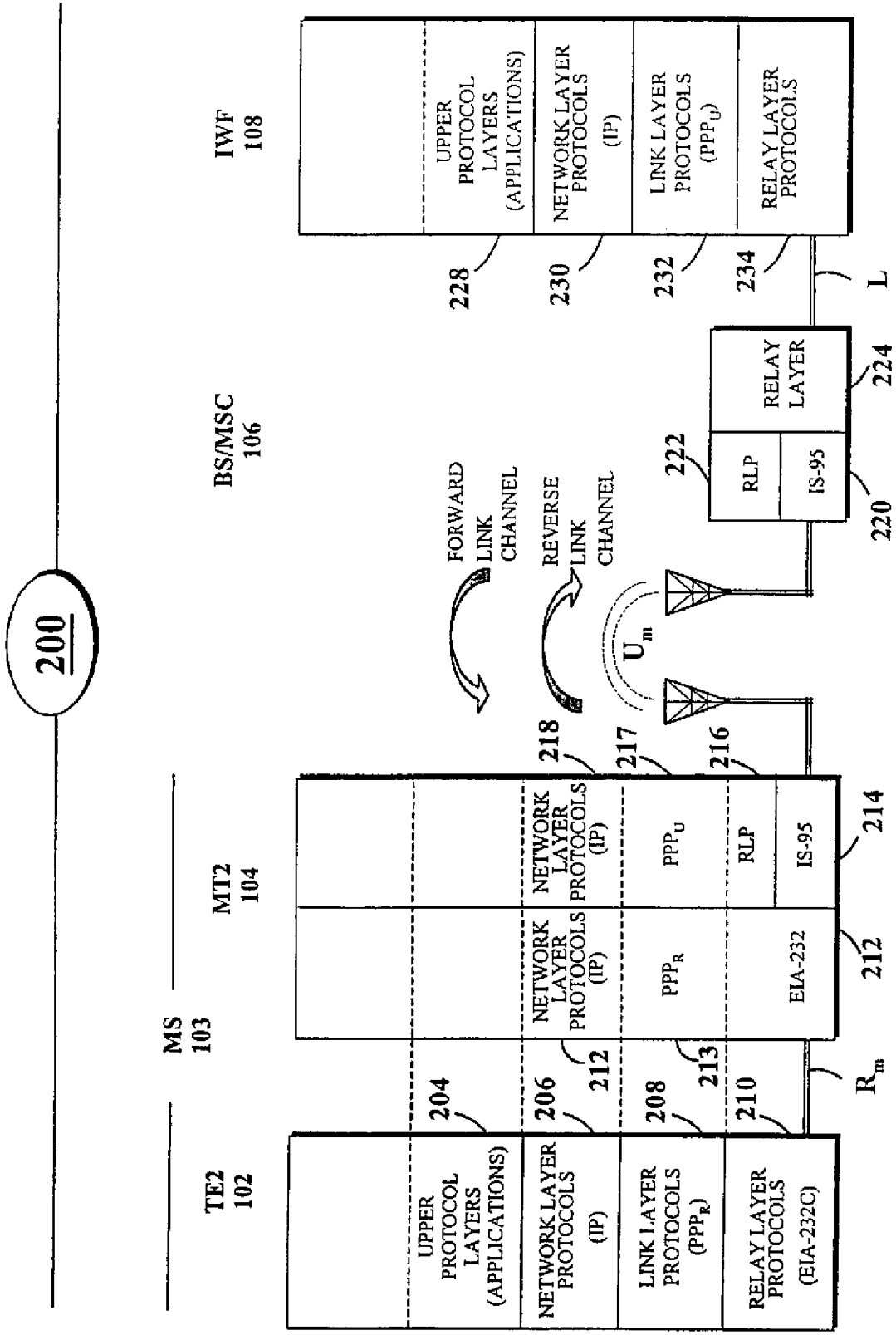

200
TE2
102
MS
103
MT2
104
BS/MSC
106
IWF
108
UPPER PROTOCOL LAYERS (APPLICATIONS)
NETWORK LAYER PROTOCOLS (IP)
LINK LAYER PROTOCOLS (PPP_R)
RELAY LAYER PROTOCOLS (EIA-232C)
204
206
208
210
212
213
R_m
NETWORK LAYER PROTOCOLS (IP)
PPP_R
EIA-232
212
NETWORK LAYER PROTOCOLS (IP)
PPP_U
RLP
IS-95
214
218
217
216
FORWARD LINK CHANNEL
REVERSE LINK CHANNEL
U_m
RLP
IS-95
222
220
RELAY LAYER
224
UPPER PROTOCOL LAYERS (APPLICATIONS)
NETWORK LAYER PROTOCOLS (IP)
LINK LAYER PROTOCOLS (PPP_U)
RELAY LAYER PROTOCOLS
228
230
232
234
L

FIG. 2

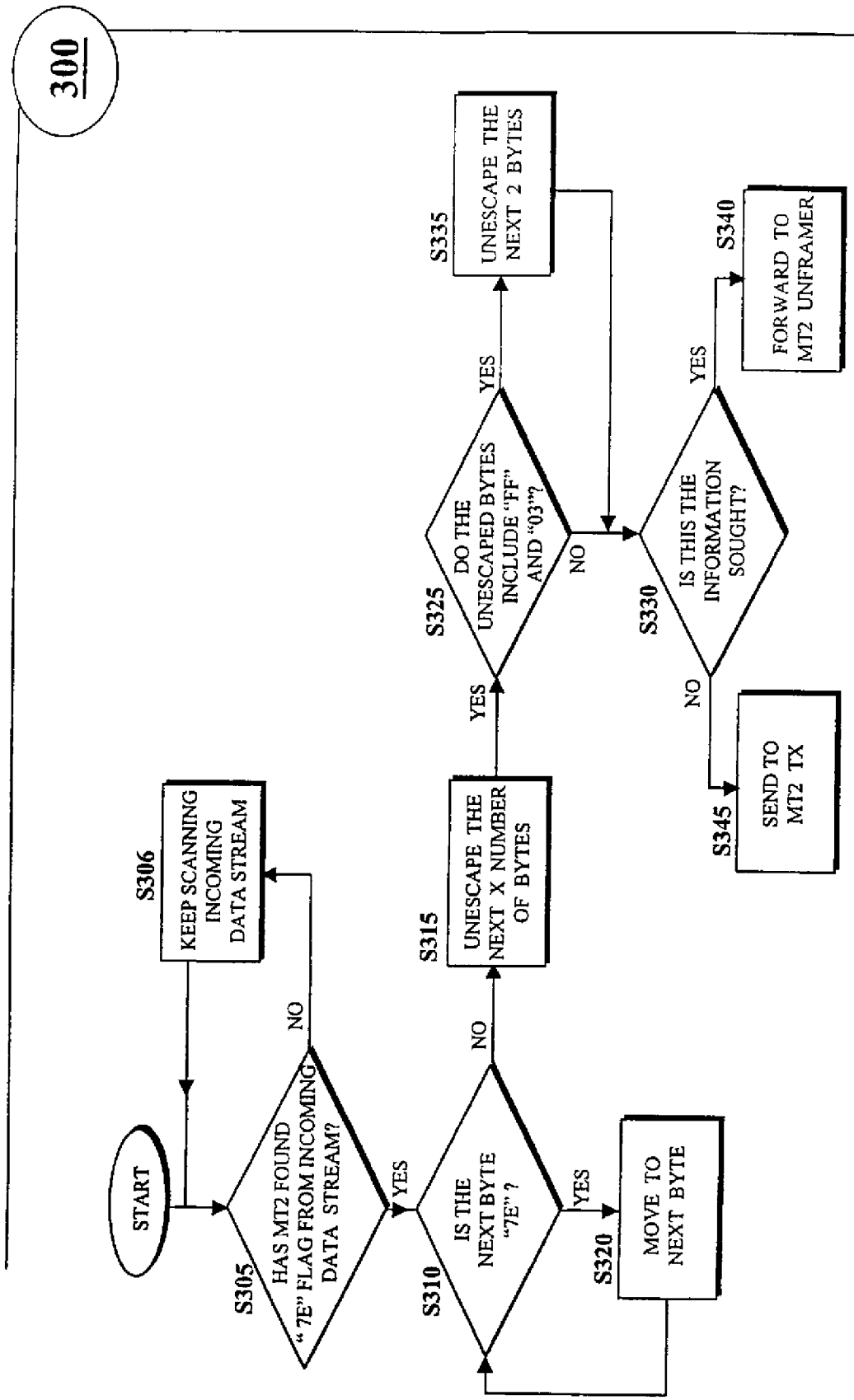

300
START
S305
HAS MT2 FOUND "7E" FLAG FROM INCOMING DATA STREAM?
NO
S306
KEEP SCANNING INCOMING DATA STREAM
YES
S310
IS THE NEXT BYTE "7E" ?
NO
S315
UNESCAPE THE NEXT X NUMBER OF BYTES
YES
S320
MOVE TO NEXT BYTE
S325
DO THE UNESCAPED BYTES INCLUDE "FF" AND "03"?
YES
S335
UNESCAPE THE NEXT 2 BYTES
NO
S330
IS THIS THE INFORMATION SOUGHT?
YES
S340
FORWARD TO MT2 UNFRAMER
NO
S345
SEND TO MT2 TX

FIG. 3

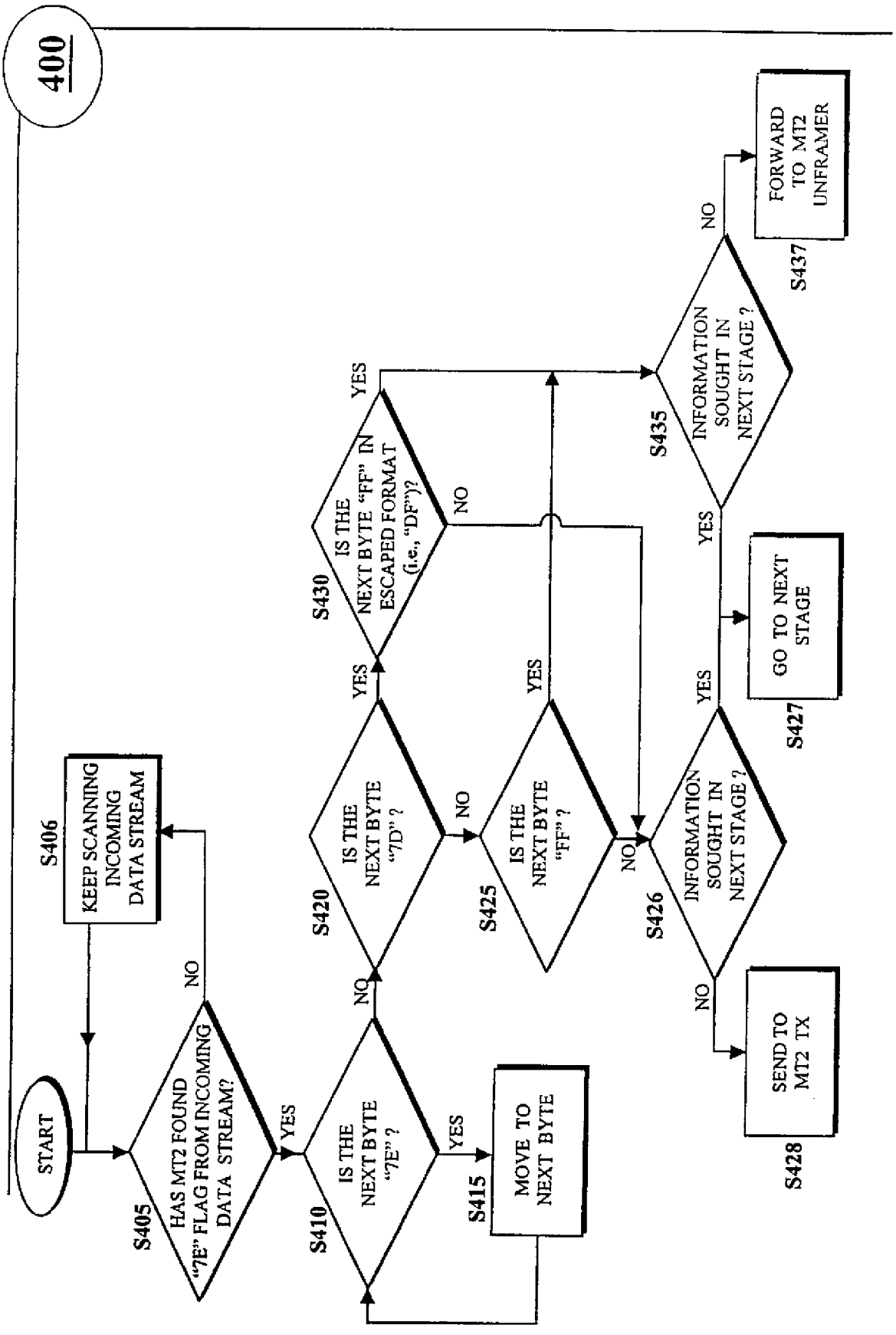

400
START
S405
HAS MT2 FOUND "7E" FLAG FROM INCOMING DATA STREAM?
NO
YES
S406
KEEP SCANNING INCOMING DATA STREAM
S410
IS THE NEXT BYTE "7E" ?
YES
S415
MOVE TO NEXT BYTE
NO
S420
IS THE NEXT BYTE "7D" ?
YES
S430
IS THE NEXT BYTE "FF" IN ESCAPED FORMAT (i.e., "DF")?
YES
NO
S435
INFORMATION SOUGHT IN NEXT STAGE ?
YES
S427
GO TO NEXT STAGE
NO
S437
FORWARD TO MT2 UNFRAMER
NO
S425
IS THE NEXT BYTE "FF" ?
YES
NO
S426
INFORMATION SOUGHT IN NEXT STAGE ?
YES
S427
GO TO NEXT STAGE
NO
S428
SEND TO MT2 TX

FIG. 4A

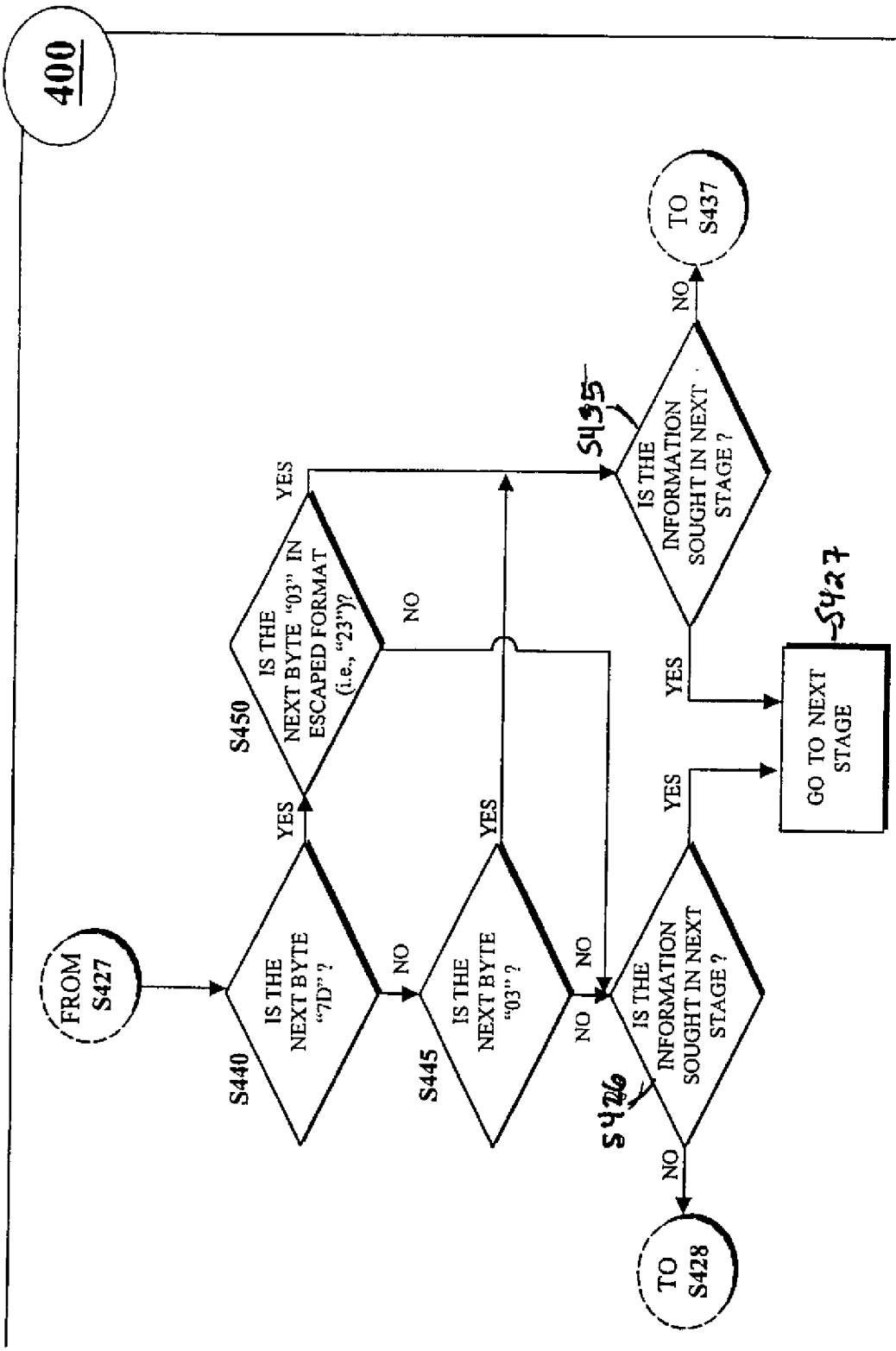

400
FROM S427
S440
IS THE NEXT BYTE "7D" ?
YES
NO
S445
IS THE NEXT BYTE "03" ?
YES
NO
S450
IS THE NEXT BYTE "03" IN ESCAPED FORMAT (i.e., "23")?
YES
NO
S426
IS THE INFORMATION SOUGHT IN NEXT STAGE ?
YES
NO
S435
IS THE INFORMATION SOUGHT IN NEXT STAGE ?
YES
NO
S427
GO TO NEXT STAGE
TO S428
TO S437

FIG. 4B

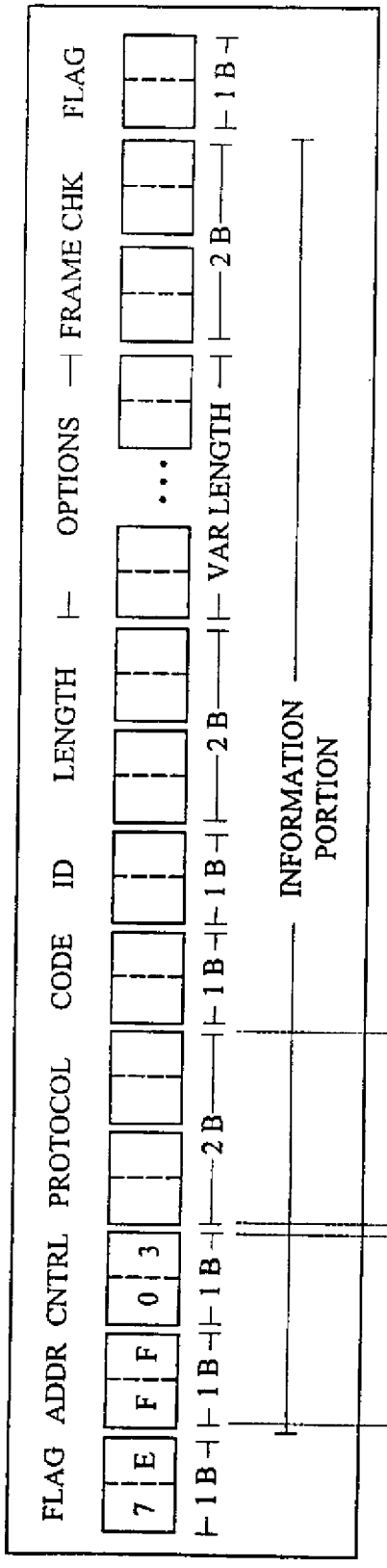

FLAG
ADDR
CNTRL
PROTOCOL
CODE
ID
LENGTH
OPTIONS
FRAME CHK
FLAG
7 E
F F
0 3
1 B
2 B
VAR LENGTH
INFORMATION PORTION
MAY BE COMPRESSED OUT
MAY BE COMPRESSED TO 1 BYTE

FIG. 5

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/19027 A3

(51) International Patent Classification[7]: H04Q 7/22, H04L 12/28

(21) International Application Number: PCT/US00/24623

(22) International Filing Date:
7 September 2000 (07.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/392,342 8 September 1999 (08.09.1999) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: **ABROL, Nischal**; 7260 Calle Cristobal, #41, San Diego, CA 92126 (US). **LIOY, Marcello**; 7588 Charmant Drive, #1924, San Diego, CA 92122 (US).

(74) Agents: **WADSWORTH, Philip, R.** et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

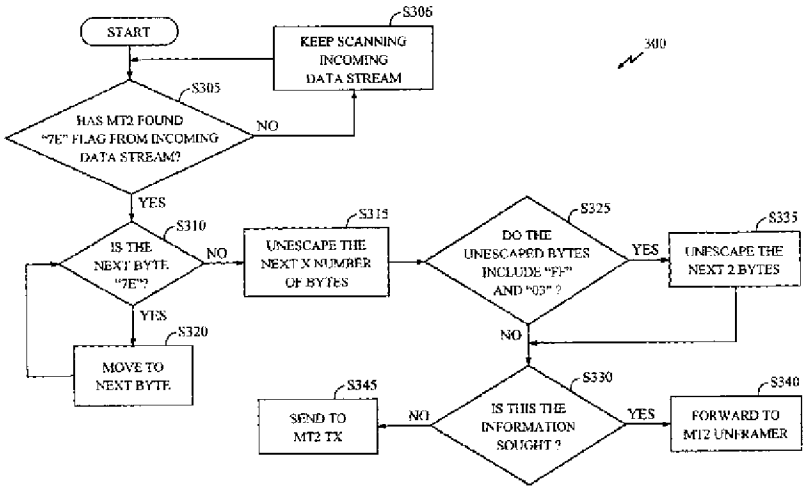
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
17 January 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHODS FOR EFFICIENT EARLY PROTOCOL DETECTION



(57) Abstract: A method and system that detects protocol and configuration messages in a PPP packet without having to unframe the entire packet. The method includes a communication device (MT2) that receives a plurality data frames (S306), wherein the communication device is capable of ascertaining the beginning of an information portion (S305) within the received frames. The communications device detects whether the information portion contains configuration information, such as protocol and configuration messages of a predetermined type. In a first embodiment, the detection is achieved by the communication device unescaping (S315) the contents of a plurality of bytes and determining (S325, S330, S335) whether the escaped bytes contains the desired configuration information. In a second embodiment, the communication device determines whether the contents of a particular byte contain the desired configuration information, in escaped or unescaped form, and the communication device continues to sequentially process the bytes within the information portion until the bytes typically containing the desired configuration information are processed.

WO 01/19027 A3

INTERNATIONAL SEARCH REPORT

Internat ...l Application No
PCT/US 00/24623

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/22 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 917 318 A (LUCENT) 19 May 1999 (1999-05-19) page 5, line 3 -page 33, line 39; figures	1-13
A	WO 96 21984 A (NOKIA) 18 July 1996 (1996-07-18) page 8, line 18 -page 17, line 22; figures	1,8
P,Y	WO 99 65178 A (ERICSSON) 16 December 1999 (1999-12-16) page 3, line 23 -page 9, line 12; figures	1,8
P,Y	WO 99 65219 A (IREADY) 16 December 1999 (1999-12-16) page 7, line 23 -page 26, line 13; figures	1,8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 July 2001	11/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Geoghegan, C

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. ial Application No
PCT/US 00/24623

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 917318 A	19-05-1999	CA 2249817 A	14-04-1999
		CA 2249830 A	14-04-1999
		CA 2249831 A	14-04-1999
		CA 2249836 A	14-04-1999
		CA 2249837 A	14-04-1999
		CA 2249838 A	14-04-1999
		CA 2249839 A	14-04-1999
		CA 2249862 A	14-04-1999
		CA 2249863 A	14-04-1999
		EP 0912026 A	28-04-1999
		EP 0910198 A	21-04-1999
		EP 0917320 A	19-05-1999
		EP 0912027 A	28-04-1999
		EP 0912012 A	28-04-1999
		EP 0917328 A	19-05-1999
		EP 0918417 A	26-05-1999
		EP 0912017 A	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999
WO 9621984 A	18-07-1996	FI 950117 A	11-07-1996
		AU 699246 B	26-11-1998
		AU 4392996 A	31-07-1996
		CA 2209944 A	18-07-1996
		EP 0804845 A	05-11-1997
		JP 10512120 T	17-11-1998
		NO 973176 A	09-09-1997
		US 5978386 A	02-11-1999
WO 9965178 A	16-12-1999	AU 4667599 A	30-12-1999
WO 9965219 A	16-12-1999	AU 4435999 A	30-12-1999
		EP 1086573 A	28-03-2001

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 2001/019027 A3

(51) International Patent Classification[7]: H04Q 7/22, H04L 12/28

(21) International Application Number: PCT/US2000/024623

(22) International Filing Date: 7 September 2000 (07.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/828,623 8 September 1999 (08.09.1999) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: ABROL, Nischal; 7260 Calle Cristobal, #41, San Diego, CA 92126 (US). LIOY, Marcello; 7588 Charmant Drive, #1924, San Diego, CA 92122 (US).

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

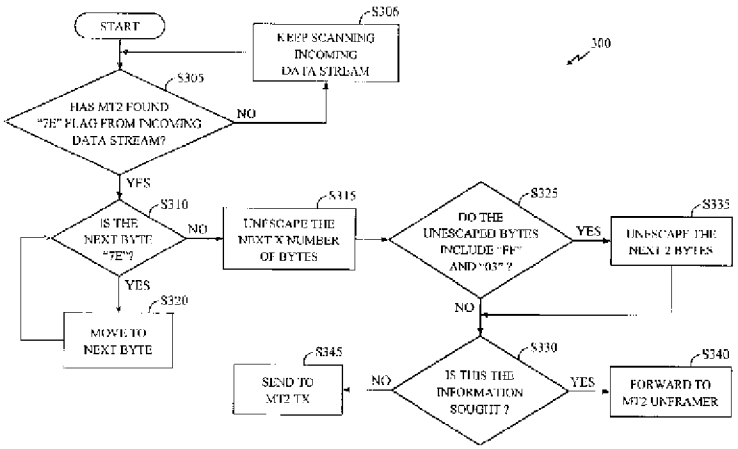
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHODS FOR EFFICIENT EARLY PROTOCOL DETECTION



(57) Abstract: A method and system that detects protocol and configuration messages in a PPP packet without having to unframe the entire packet. The method includes a communication device (MT2) that receives a plurality data frames (S306), wherein the communication device is capable of ascertaining the beginning of an information portion (S305) within the received frames. The communications device detects whether the information portion contains configuration information, such as protocol and configuration messages of a predetermined type. In a first embodiment, the detection is achieved by the communication device unescaping (S315) the contents of a plurality of bytes and determining (S325, S330, S335) whether the escaped bytes contains the desired configuration information. In a second embodiment, the communication device determines whether the contents of a particular byte contain the desired configuration information, in escaped or unescaped form, and the communication device continues to sequentially process the bytes within the information portion until the bytes typically containing the desired configuration information are processed.

WO 2001/019027 A3

(88) Date of publication of the international search report:
17 January 2002

(48) Date of publication of this corrected version:
31 December 2003

(15) Information about Corrections:
see PCT Gazette No. 01/2004 of 31 December 2003, Section II

Previous Correction:
see PCT Gazette No. 40/2002 of 3 October 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/019027 A3

(51) International Patent Classification[7]: H04Q 7/22, H04L 12/28

(21) International Application Number: PCT/US00/24623

(22) International Filing Date:
7 September 2000 (07.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/392,342 8 September 1999 (08.09.1999) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: ABROL, Nischal; 7260 Calle Cristobal, #41, San Diego, CA 92126 (US). LIOY, Marcello; 7588 Charmant Drive, #1924, San Diego, CA 92122 (US).

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

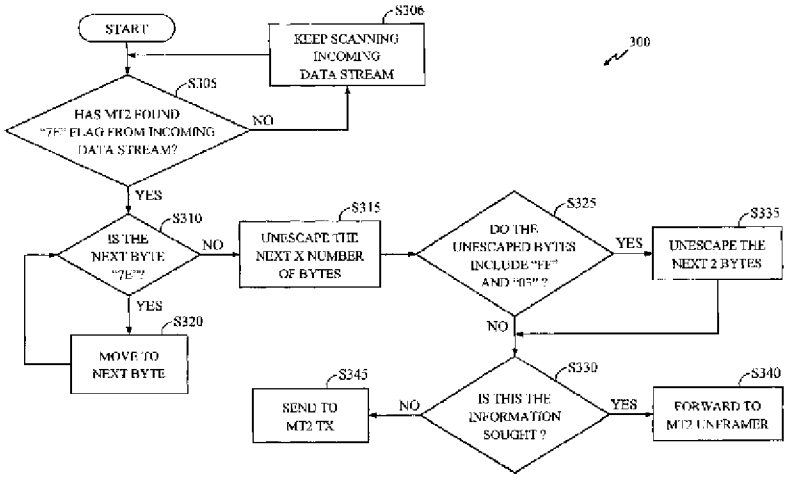
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHODS FOR EFFICIENT EARLY PROTOCOL DETECTION



(57) Abstract: A method and system that detects protocol and configuration messages in a PPP packet without having to unframe the entire packet. The method includes a communication device (MT2) that receives a plurality data frames (S306), wherein the communication device is capable of ascertaining the beginning of an information portion (S305) within the received frames. The communications device detects whether the information portion contains configuration information, such as protocol and configuration messages of a predetermined type. In a first embodiment, the detection is achieved by the communication device unescaping (S315) the contents of a plurality of bytes and determining (S325, S330, S335) whether the escaped bytes contains the desired configuration information. In a second embodiment, the communication device determines whether the contents of a particular byte contain the desired configuration information, in escaped or unescaped form, and the communication device continues to sequentially process the bytes within the information portion until the bytes typically containing the desired configuration information are processed.

WO 01/019027 A3

(88) Date of publication of the international search report:
17 January 2002

(48) Date of publication of this corrected version:
3 October 2002

(15) Information about Correction:
see PCT Gazette No. 40/2002 of 3 October 2002, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHODS FOR EFFICIENT EARLY PROTOCOL DETECTION

BACKGROUND OF THE INVENTION

I. Field of the Invention

This invention generally relates to the field of wireless communications. More particularly, the present invention relates to a novel method and system for performing early protocol and configuration message detection without having to unframe entire PPP packets.

II. Description of Related Art

Recent innovations in wireless communication and computer-related technologies, as well as the unprecedented growth of Internet subscribers, have paved the way for mobile computing. In fact, the popularity of mobile computing has placed greater demands on the current Internet infrastructure to provide mobile users with more support. A crucial part of meeting these demands and providing users with the necessary support is the use of Code Division Multiple Access (CDMA) technology in wireless communication systems.

CDMA is a digital radio-frequency (RF) channelization technique defined in the Telecommunications Industry Association/Electronics Industries Association Interim Standard-95 (TIA/EIA IS-95), entitled "MOBILE STATION-BASE STATION COMPATIBILITY STANDARD FOR DUAL-MODE WIDEBAND SPREAD SPECTRUM CELLULAR SYSTEM", published in July 1993 and herein incorporated by reference. Wireless communication systems employing this technology assign a unique code to communication signals and spread these communication signals across a common (wideband) spread spectrum bandwidth. As long as the receiving apparatus in a CDMA system has the correct code, it can successfully detect and select its communication signal from the other signals concurrently transmitted over the same frequency band. The use of CDMA produces an increase in system

traffic capacity, improves overall call quality and noise reduction, and provides a reliable transport mechanism for data service traffic.

FIG. 1 illustrates the basic elements of such a wireless data communication system **100**. Artisans of ordinary skill will readily appreciate that these elements, or their interfaces, may be modified, augmented, or subjected to various standards known in the art, without limiting their scope or function. System **100** allows a mobile terminal equipment, TE2 device **102** (e.g., the terminal equipment such as laptop or palmtop computer) to communicate with an Interworking Function (IWF) **108**. System **100** includes a wireless communication device, MT2 device **104** (e.g., wireless telephone), and a Base Station/Mobile Switching Center (BS/MSC) **106**. The IWF **108** serves as a gateway between the wireless network and other networks, such as the Public Switched Telephone Network or wireline packet data networks providing Internet- or Intranet-based access.

As shown in FIG. 1, the IWF **108** is coupled to the BS/MSC **106**, via the L interface. Often the IWF **108** will be co-located with the BS/MSC **106**. The TE2 device **102** is electronically coupled to the MT2 device **104** via the R_m interface. The MT2 device **104** communicates with the BS/MSC **106** via the wireless interface U_m. The TE2 device **102** and the MT2 device **104** may be integrated into a single unit or may be separated out, as in the case of an installed mobile phone unit in which a laptop is the TE2 device **102** and the transceiver is the MT2 device **104**. It is important to note that, as indicated by FIG. 2, the combination of the TE2 device **102** and the MT2 device **104**, whether integrated or separate, is generally referred to as a mobile station (MS) **103**.

Other support is made possible by applying various well-known protocols to control, manage, or otherwise facilitate different aspects of wireless communications. For example, the life-blood of the Internet infrastructure, the Internet Protocol (IP), has been incorporated in wireless communications to accommodate packet-oriented services. The IP protocol specifies the addressing and routing of packets (datagrams) between host computers and is defined in Request For Comment 791 (RFC 791) entitled, "INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL

SPECIFICATION," published September 1981, and herein incorporated by reference.

The IP protocol is a network layer protocol that encapsulates data into IP packets for transmission. Addressing information is affixed to the header of the packet. IP headers (e.g., IP version 4) contain 32-bit addresses that identify the sending and receiving hosts. These addresses are used by intermediate routers to select a path through the network for the packet towards its ultimate destination at the intended address. Thus, the IP protocol allows packets originating at any Internet node in the world to be routed to any other Internet node in the world, given that the originating party knows the IP address of the destination party.

Another well-known protocol which has been incorporated in wireless communications systems is the Point-to-Point Protocol (PPP) protocol, which provides, *inter alia*, Internet access. The PPP protocol is described in detail in Request for Comments 1661 (RFC 1661), entitled "THE POINT-TO-POINT PROTOCOL (PPP)", published July 1994 and herein incorporated by reference.

Essentially, the PPP protocol specifies a method for transporting multi-protocol datagrams over point-to-point links and contains three main components: a method of encapsulating multi-protocol datagrams over serial links; a Link Control Protocol (LCP) for establishing, testing, configuring, and maintaining a data link connection; and a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

In an effort to provide a host of services on wireless communication systems, various standards have been developed to accommodate the wireless data transmission between the TE2 device **102** and the IWF **108**. For example, the TIA/EIA IS-707.5 standard, entitled "DATA SERVICE OPTIONS FOR WIDEBAND SPREAD SPECTRUM SYSTEMS: PACKET DATA SERVICES," published February 1998, and herein incorporated by reference, defines requirements for support of packet data transmission capability on TIA/EIA IS-95 systems and specifies a suite of packet data bearer services. Similarly, the TIA/EIA IS-707-A.5 standard, entitled "DATA

SERVICE OPTIONS FOR SPREAD SPECTRUM SYSTEMS: PACKET DATA SERVICES," and the TIA/EIA IS-707-A.9 standard, entitled "DATA SERVICE OPTIONS FOR SPREAD SPECTRUM SYSTEMS: HIGH-SPEED PACKET DATA SERVICES," both published in March 1999 and incorporated by reference, also define requirements for packet data transmission support on TIA/EIA IS-95 systems.

These standards provide that certain packet data service options that may be used to communicate between the TE2 device **102** and IWF **108** via BS/MSC **106**. In doing so, IS-707.5 introduces the Network Model, which details the packet data protocol requirements for the R_m interface, U_m interface, and the L interface. Under this model, two separate PPP links are provided at the data link layer: a first PPP link (PPP_R) provides the data link layer between the TE2 device **102** and the MT2 device **104** (i.e., across the R_m interface), and a second PPP link (PPP_U), independent of the first, provides the data link layer between the MT2 device **104** and the IWF **108** (i.e., across the U_m and L interfaces).

The separate and independent PPP links help support "transparent mobility"; that is, the TE2 device **102** should experience seamless and transparent service, regardless of time and its current IWF **108** point-of-attachment. As such, the TE2 device **102** should not be affected by location changes. For example, the TE2 device **102** should not be affected from PPP renegotiations occurring on the U_m link, such as when MT2 device **104** attempts to attach to a different IWF **108**. Thus, the Network Model operates to isolate the PPP_R link from the PPP_U link in order to prevent changes on the U_m link from affecting the R_m link. In other words, the PPP_U link can be renegotiated without forcing the PPP_R link to be renegotiated.

FIG. 2 illustrates the protocol stacks in each entity of the IS-707.5 Network Model. At the far left of FIG. 2 is a protocol stack, shown in conventional vertical format, depicting the protocol layers running on the TE2 device **102** (e.g., the mobile terminal, laptop or palmtop computer). The TE2 device **104** protocol stack is illustrated as being logically connected to the MT2 device **104** protocol stack over the R_m interface. The MT2 device **104**, is illustrated as being logically connected to the BS/MSC **106** protocol stack

over the U_m interface. The BS/MSC **106** protocol stack is, in turn, shown as being logically connected to the IWF **108** protocol stack over the L interface.

By way of example, the protocols depicted in FIG. 2, operate as follows: the PPP_R protocol **208** on the TE2 **102** device encodes packets from the upper layer protocols **204**, and the network layer IP protocol **206**. The PPP_R protocol **208** then transmits the packets across the R_m interface using the TIA/EIA 232-F protocol **210** to the TIA/EIA-232-F-compatible port on the MT2 device **104** running the TIA/EIA 232-F protocol **212**. The TIA/EIA-232-F standard is defined in "INTERFACE BETWEEN DATA TERMINAL EQUIPMENT AND DATA CIRCUIT-TERMINATING EQUIPMENT EMPLOYING SERIAL BINARY DATA INTERCHANGE", published in October 1997 and herein incorporated by reference. It is to be understood that other standards or protocols known to artisans of ordinary skill in the art may be used to define the transmission across the R_m interface. For example, other applicable R_m interface standards include, the "UNIVERSAL SERIAL BUS (USB) SPECIFICATION, Revision 1.1", published in September 1998, and the "BLUETOOTH SPECIFICATION VERSION 1.0A CORE, published in July 1999, both incorporated by reference.

The TIA/EIA 232-F protocol **212** on the MT2 device **104** receives the packets from the TE2 device **102** and passes them to the PPP_R protocol **213**. As stated above, the PPP_R protocol **213** unframes the packets encapsulated in the PPP frames and typically, when a data connection is up, the protocol **213** transfers the packets to PPP_U protocol **217**. Protocol **217** essentially re-frames the packets for transmission to a PPP_U peer located in the IWF **108**. The Radio Link Protocol (RLP) **216** and IS-95 protocol **214**, both of which are well known in the art, are used to transmit the packet-encapsulated PPP frames to the BS/MSC **106** over the U_m interface. The RLP protocol **216** is defined in the IS-707.2 standard, entitled "DATA SERVICE OPTIONS FOR WIDEBAND SPREAD SPECTRUM SYSTEMS: RADIO LINK PROTOCOL", published in February 1998 and herein incorporated by reference, as well as the IS-707-A.2 standard, entitled "DATA SERVICE OPTIONS FOR SPREAD SPECTRUM SYSTEMS: RADIO LINK PROTOCOL", published in March 1999 and also incorporated by reference.

A corresponding RLP protocol **220** and IS-95 protocol **222** in the BS/MSC **106** transfer the packets to the relay layer protocol **224** for transmission across the L interface to the relay layer protocol **224** on the IWF **108**. The PPP_U protocol **232** then unframes the received packets and transfers them to the network layer protocol IP **230**, which in turn passes them to the upper layer protocols **228** or forwards them to the Internet.

As stated above, the PPP_R protocol **213** transfers the packets to the PPP_U protocol **217** when a data link connection is established. RFC 1661 provides that Link Control Protocol (LCP) packets must be exchanged and negotiated over each PPP link (i.e., PPP_R and PPP_U) in order to establish, configure, and test the data link connection. As such, these LCP packets comprise Configure-Request, Configure-Ack, Configure-Nak, Protocol-Reject, and Configure-Reject messages to negotiate various options and operate as follows: the Configure-Request packet is used to negotiate configuration options. The Configuration-Ack packet is only transmitted if every configuration option in a received Configuration-Request packet is recognizable and all values are acceptable. The Configure-Nak packet is sent when the requested configuration options in a Configuration-Request packet are recognizable but contain values that are not acceptable and the Configure-Nak Options field is filled with the unacceptable Configure-Request configuration options and suggested values that will work. The Configure-Reject packet is sent when the requested configuration options in a Configure-Request includes configuration options that are not understood by the receiver and the Configure-Reject Options field contains the unrecognized Configure-Request configuration options.

Once the LCP packets are exchanged, the link options negotiated, and the data link connection established, a network layer connection must be established between the TE2 device **102** and the IWF **108**. Such a connection is achieved through protocols **206, 212, 218, 230**, which include, for example, the IP protocol. The negotiating, configuring, enabling, and disabling of the IP protocol on both ends of the PPP links is provided by the Internet Protocol Control Protocol (IPCP). IPCP is a part of a family of Network Control Protocols (NCPs) included in the PPP protocol and is described in Request for

Comment (RFC) 1332, "THE PPP INTERNET PROTOCOL CONTROL PROTOCOL (IPCP)", published in May 1992 and herein incorporated by reference.

The IPCP protocol uses the same configuration option negotiation mechanism as the LCP protocol and, much like the LCP protocol, IPCP negotiations occur separately for both the R_m interface and the U_m interface. As described in RFC 1661, the Configuration-Ack packet contains a list of the options, which the Sender is acknowledging. The MT2 device **104** monitors the received and transmitted Configuration-Ack packets over the R_m and U_m interfaces and stores the value of each option in a storage device, such as a computer memory. All configuration options have default values, defined by RFC 1661, which are used when the corresponding configuration option is not negotiated. It is to be noted that the configuration option default values may be defined by other RFCs, such as, for example, RFC 1877 entitled "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses" published in December 1995 and incorporated by reference.

As stated above with respect to the Network Model, the PPP_U link can be renegotiated without forcing the PPP_R link to be renegotiated. To maintain such isolation between the R_m and U_m interfaces, the MT2 device **104** generally unframes and reframes received PPP packets. Unless packets received by the MT2 device **104** are to be passed to an executing upper layer protocol within the MT2 device **104**, the PPP packets are unframed only to be reframed for subsequent transmission to a PPP peer protocol. This unframing/reframing occurs even when the packets require no further processing in the MT2 device **104**. For example, when a call is initially brought up, the LCP and IPCP mechanisms can negotiate to establish identical configuration options for both the U_m and R_m interfaces. As long as the configuration options remain identical, all of the PPP data packets (as opposed to the configuration packets) could "pass through", from one interface to the other, without the MT2 device **104** unframing/reframing the packets. Clearly, in cases where the configuration options remain identical, the MT2 device **104** performs too many unnecessary PPP packet

unframing/reframing operations. Such operations adversely affect the processing resources and throughput latency of the MT2 device **104**.

However, if the configuration options change, they must be renegotiated, which militates in favor of unframing/reframing the PPP packets. For example, by virtue of the fact that the MT2 device **104** is mobile, it is capable of moving to an area that is served by an IWF **108** that is different from the original IWF **108**. When this happens, the MT2 device **104** will be "handed off" to the new IWF **108** for service. This handoff requires the renegotiation of particular LCP and IPCP configuration options over the U_m interface as well as the intervention of the MT2 device **104**. If the packets containing the configuration option messages (e.g., Configure-Request, Configure-Ack, Configure-Nak, etc.) were simply "passed through", without unframing or examining the contents of the packets, the packets would force the end-to-end resynchronization of the entire link which would terminate the independence of the R_m and U_m links.

Therefore, what is needed is a novel and efficient method and system capable of early protocol and configuration message detection without having to unframe a PPP packet.

SUMMARY OF THE INVENTION

The present invention addresses the need identified above by providing a method and system that detects protocol and configuration messages in a PPP packet without having to unframe the entire packet.

Methods and systems consistent with the principles of the present invention as embodied and broadly described herein include a communication device that receives a plurality data frames, wherein the communication device is capable of ascertaining the beginning of an information portion within the received frames. The communications device detects whether the information portion contains configuration information, such as protocol and configuration messages of a predetermined type. In a first embodiment, the detection is achieved by the communication device unescaping the contents of a plurality of bytes and

determining whether the escaped bytes contains the desired configuration information. In a second embodiment, the communication device determines whether the contents of a particular byte contain the desired configuration information, in escaped or unescaped form, and the communication device continues to sequentially process the bytes within the information portion until the bytes typically containing the desired configuration information are processed or it is determined that the information does not exist.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this Specification, illustrate an embodiment of the invention and, together with the description, explain the objects, advantages, and principles of the invention. In the drawings:

FIG. 1 is a high level block diagram depicting various elements of a wireless communication system.

FIG. 2 schematically describes the protocol stacks of a wireless communication system.

FIG. 3 is a flow-chart diagrams describing a first embodiment of the invention.

FIGS. 4A, 4B are flow-chart diagrams describing a second embodiment of the invention.

FIG. 5 describes the general format of a packet encapsulated in a PPP frame.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The following detailed description of the embodiments of the present invention refers to the accompanying drawings that illustrate these. Other embodiments are possible and modifications may be made to the embodiments without departing from the spirit and scope of the invention.

Therefore, the following detailed description is not meant to limit the invention. Rather the scope of the invention is defined by the appended claims.

It will be apparent to one of ordinary skill in the art that an embodiment of the present invention, as described below, may be realized in a variety of implementations, including the software, firmware, and hardware of the entities illustrated in the figures (i.e., TE2 device **102**, MT2 device **104**, BS/MSC **106** and IWF **108**). The actual software code or control hardware used to implement the present invention is not limiting of the present invention. Thus, the operation and behavior of the present invention will be described without specific reference to the actual software code or hardware components. Such non-specific references are acceptable because it is clearly understood that a person of ordinary skill in the art would be able to design software and control hardware to implement the embodiment of the present invention based on the description herein.

Because the embodiments described herein operate on PPP packets encapsulated in HDLC frames, FIG. 5 illustrates the various attributes of such packets. The beginning (and end) of the frame is demarcated by a 1-byte framing flag represented by the hexadecimal character "7E". The following two bytes indicate the protocol address and control field which, for standard PPP packets, are typically designated as the hexadecimal characters "FF" and "03", respectively. The next two bytes indicate the protocol type, such as, for example, the LCP protocol, denoted by the hexadecimal characters "C0" and "21"; the IPCP protocol, indicated by the hexadecimal characters "80" and "21"; or the Van Jacobson protocol compressed state, indicated by the hexadecimal characters "00" (which may be compressed out) and "2D". The subsequent byte indicates the code or the configuration message, such as Configure-Request, denoted by the hexadecimal character "01"; Configure-Ack, indicated by the hexadecimal character "02"; or Configure-Nak, indicated by the hexadecimal character "03".

1. **First Embodiment**

FIG. 3 is a flow-chart diagram depicting a first embodiment of the present invention. As such, FIG. 3 details the operation of the MT2 device **104** for performing early protocol and configuration message detection in PPP packets.

In step **S305**, the MT2 device **104**, first scans an incoming data stream to detect the framing flag, indicated by the hexadecimal character "7E". This flag demarcates a frame and can, therefore, be used to indicate the beginning and/or end of packets encapsulated in PPP frames. If the MT2 device **104** has not detected a "7E" framing flag, it keeps scanning the incoming data, as indicated by step **S306**, until it detects the flag. Once the MT2 device **104** detects the "7E" framing flag, it progresses to step **S310**.

After detecting a "7E" flag, the MT2 device **104**, in step **S310**, determines whether the next byte is also a "7E" flag. If so, the MT2 device **104** skips that particular byte, as indicated in step **S320**, and returns back to step **S310** to apply the "7E" flag test to the next byte. If the next byte is not a "7E" flag, the MT2 device **104** progresses to step **S315**. It is important to note that the incoming data stream may contain consecutive "7E" flags, as in the case of back-to-back packets where a "7E" flag, indicating the end of a frame, is juxtaposed to a subsequent "7E" flag, indicating the beginning of a new frame. Steps **S310** and **S320** operate to filter out the framing flags, enabling the MT2 device **104** to discern where the information portion of the framed packet begins.

Aware that the next byte is not a "7E" flag, but an information byte, the MT2 device **104** in step **S315**, "unescapes" the next X number of bytes, where X corresponds to the relative position of the information sought within the framed-packet. This unescaping is performed because, as is well known in the art, when the PPP protocol is transmitted with asynchronous, HDLC-like framing (i.e., as per RFC 1662), the protocol employs an "escaping technique" to mask certain characters within the information portion of a packet that also function as special control characters. Such characters include the aforementioned "7E" flag as well as the escape flag "7D". When these characters are encountered in the information portion of a framed-

packet, the escaping technique stuffs the escape flag "7D" in front of the character and modifies the character in order to neutralize its control function. Therefore, in seeking to detect certain protocol or configuration information from an incoming data stream, the MT2 device **104**, in step **S315**, unescapes the number of bytes necessary to access the information sought in order to uncover its true identity. After unescaping X bytes, the MT2 device **104** proceeds to step **S325**.

In step **S325**, the MT2 device **104** determines whether the unescaped X bytes include the standard PPP address and control field characters "FF" and "03", respectively. Although these characters typically comprise the first and second bytes of the information portion of a PPP packet (*see, e.g.*, FIG. 5), these characters may be compressed out of the packet, thereby affecting the location of the ensuing information bytes. Therefore, the MT2 device **104** must check whether these characters are included within the unescaped bytes of the packet in order to make the necessary adjustments later. If the characters "FF" and "03" are not included in the unescaped bytes (i.e., characters "FF" and "03" are compressed out), the MT2 device **104**, in step **S330**, checks to see whether these bytes contain the protocol or configuration message information being sought. If they do, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer, in order to unframe the packet and engage in the processing indicated by the detected information. If the bytes do not contain the information being sought, the MT2 device **104** sends the entire packet to the MT2 device **104** transmit portion to be forwarded across the pertinent interface, as indicated by step **S345**.

Returning to step **S325**, if the unescaped X bytes include "FF" and "03", the MT2 device **104**, in step **S335**, compensates by unescaping another 2 bytes, in addition to the specified X bytes. This adjusts for the inclusion of the "FF" and "03" characters within the X bytes. The MT2 device **104** then submits the X + 2 unescaped bytes to step **S330**, where, as stated above, it checks to see whether the unescaped bytes contain the desired information. If they do, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer. If the bytes do not contain the protocol or

configuration message information being sought, the MT2 device **104**, in step **S345**, sends the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface.

To illustrate the operation of this embodiment, suppose the early detection of an LCP protocol packet is desired. The LCP protocol specification is provided within the protocol information portion of a PPP-framed packet. As indicated in FIG. 5, the protocol information is 2 bytes long, typically occupying byte positions 3 and 4 of the information portion of a standard PPP-framed packet. After scanning the incoming data stream and discerning where the information bytes begin (i.e., steps **S305**, **S310**, and **S320**), the MT2 device **104** unescapes the next two bytes (i.e., X equal to 2), as indicated by step **S315**. If, in step **S325**, the first 2 bytes do not include the "FF" and "03" characters, then the MT2 device **104** checks to see whether these bytes contain the LCP information being sought. If it does, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer, in order to unframe the packet and engage in the processing required by the LCP protocol information. If the bytes do not contain the LCP information, the MT2 device **104** sends the entire packet to the MT2 device **104** transmit portion to be forwarded across the pertinent interface, as indicated by step **S345**.

If, on the other hand, the first two bytes of the unescaped X bytes are "FF" and "03", the MT2 device **104**, in step **S335**, compensates by unescaping the next 2 bytes, in addition to the first two bytes. The MT2 device **104** then submits all four unescaped bytes to step **S330**, where, as stated above, it checks to see whether these bytes contain the LCP information being sought. If they do, then the MT2 device **104**, in step **S340**, forwards the entire packet to the MT2 device **104** unframer. If the bytes do not contain the LCP information, the MT2 device **104**, in step **S345**, sends the entire packet to the MT2 device **104** transmit portion.

It is important to note that, by virtue of the embodiment described above, all of the header information contained within the PPP-framed packet can be detected without unframing the entire packet. For example, by simply adjusting the X value in step **S315**, this embodiment can detect such

PPP information as protocol information, configuration messages, packet ID, etc.

Thus, this embodiment detects protocol and configuration messages within a PPP packet stream without having to unframe the entire packets. Rather, by unescaping certain bytes within the information portion of the packets, this embodiment provides a system and method that efficiently detects protocol and configuration messages without performing unnecessary PPP packet unframing/reframing operations.

2. **Second Embodiment**

FIGS. 4A, 4B are flow-chart diagrams depicting a second embodiment of the present invention. This embodiment detects protocol and configuration messages contained within the information portion of a PPP-framed packet by scanning the incoming data stream and mechanically checking the information bytes in stages, without unframing the packets. Given the format of the PPP-framed packets, as illustrated by FIG. 5, the first stage specifically detects the content of the 1-byte address field, contained within the information portion of the packet. The second stage is directed to detecting the contents of the 1-byte control field, which follows the address field. Accordingly, this embodiment is capable of advancing the stages, and detecting the contents of all information fields, until the end of the information portion. For example, a third stage could be directed to detecting the contents of the 2-byte protocol field, which follow the control field. However, because of the PPP-framed packet structure and the sequential nature of this embodiment, information contained in the later fields of the frame, is generally detected after processing and detecting information contained in the preceding fields.

As a representative example of this embodiment, suppose the information sought is contained within the control field. To access this field and detect the pertinent information from an incoming data stream, the MT2 device **104** must first identify the beginning of the information portion of the PPP packet and then access and detect the information in the address

field. Only after processing the address field information, is the MT2 device **104** ready to access and detect the control field information.

As such, FIG. 4A illustrates the first stage of this embodiment. In step **S405**, the MT2 device **104** first scans the incoming data stream to detect the framing flag "7E". After detecting the "7E" flag, the MT2 device **104**, in step **S410**, determines whether the next byte is also a "7E" flag. If it is, the MT2 device **104** moves to the next byte, as indicated in step **S415**, and returns back to step **S410** to apply the "7E" flag test to the next byte. If the next byte is not a "7E" flag, the MT2 device **104** progresses to step **S420**. As stated above with respect to the first embodiment, steps **S410** and **S415** operate to filter out the framing flags, allowing the MT2 device **104** to identify the beginning of the information portion of the PPP-framed packet.

Once the MT2 device **104** is able to identify the beginning information portion, it exploits the format of PPP packets to detect the information in stages. As stated above, the first stage of this embodiment is to detect the character "FF".

In step **S420**, the MT2 device **104** checks to see whether the first information byte is the escape character "7D". As indicated above, the escaping technique stuffs the escape flag "7D" in front of certain characters and masks them. If the first information byte is not "7D" (i.e., the first information byte is not escaped), the MT2 device **104**, in step **S425**, checks to see if the first information byte is the "FF" character (i.e., in unescaped form). If it is, the MT2 device **104** proceeds to step **S435**. If first information byte is not the "FF" character, the MT2 device **104** determines, in step **S426**, whether there is more information within the framed-packet to be sought, and if there is, the MT2 device **104** moves onto the next stage in step **S427**. If there is no additional desired information, the MT2 device **104**, in step **S428**, sends the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface.

Returning to step **S420**, if the first information byte is "7D" (i.e., the first information byte is escaped), the MT2 device **104**, in step **S430**, checks to see whether the next byte is the "FF" character in the escaped format (i.e., hexadecimal character "DF"). If it is, the MT2 device **104** proceeds to step

S435. If the next byte is not the "DF" character, the MT2 device **104** proceeds to step **S426** where, as stated above, the MT2 device **104** checks to see whether there is more desired information. If there is, the MT2 device **104** moves onto the next stage in step **S427**. If there is no additional desired information, the MT2 device **104**, in step **S428**, sends the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface.

If, in step **S430**, the next byte is the "FF" character in the escaped format (i.e., hexadecimal character "DF"), the MT2 device **104** proceeds to step **S435**, where it checks to see whether there is more information to be sought. If there is, the MT2 device **104** moves onto the next stage in step **S427**. If there is no additional desired information, the MT2 device **104**, in step **S437**, forwards the entire packet to the MT2 device **104** unframer, in order to unframe the packet and engage in the processing indicated by the detected information.

After completing the first stage of the embodiment (i.e., the detection of the "FF" character in the protocol address field), the MT2 device **104** must, consistent with the object of the representative example, endeavor to detect the "03" character in the control field. As noted above, this detection is referred to as the second stage detection for this embodiment and is depicted in FIG. 4B.

Upon completing the first stage, as indicated by step **S427**, the MT2 device **104**, in step **S440**, determines, once again, whether the next byte is the "7D" character. As stated above, this determination is used in case the characters within the relevant information field were escaped. If the next byte is not the "7D" character, the MT2 device **104**, in step **S445**, determines whether the byte is the "03" character (i.e., in unescaped format). If it is, the MT2 device **104** progresses to step **S435** where, as previously noted, the MT2 device **104** determines whether there is additional information being sought, and if there is the MT2 device **104** moves onto the next stage, as per step **S427**. Otherwise, the MT2 device **104**, in step **S428**, forwards the entire packet to the MT2 device **104** transmit portion to forward the packet across the relevant interface.

Returning to step **S440**, if the MT2 device **104** determines that the following byte is the "7D" character, it checks to see, in step **S450**, whether the subsequent byte is the "03" character in the escaped format (i.e., hexadecimal character "23"). If the subsequent byte is not the "23" character, the MT2 device **104** proceeds to step **S426**, to determine whether to move onto the next stage, as in step **S427**, or send the entire packet to the MT2 device **104** transmit portion to forward the packet across the pertinent interface, as in step **S428**. If the subsequent byte is the "23" character, the MT2 device **104** proceeds to step **S435** where it determines whether to move onto the next stage, as in step **S427**, or forward the entire packet to the MT2 device **104** unframer, as in step **S437**.

Thus, this embodiment detects protocol and configuration messages within a PPP packet stream without having to unframe the packets. Rather, this embodiment scans the incoming data stream and mechanically checks the information bytes in stages. These stages correspond to the information fields of the PPP-framed packets and, therefore, this embodiment detects the desired information sequentially without performing unnecessary PPP packet unframing/reframing operations and without ignoring messages affecting link configurations.

The foregoing description of preferred embodiments of the present invention provides illustration and description, but is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible consistent with the above teachings or may be acquired from practice of the invention. Accordingly, the scope of the invention is defined by the claims and their equivalents.

What is claimed is:

CLAIMS

1. A method for early detection of configuration information of a predetermined type, said method comprising:

receiving, on a communication device, a plurality of framed data packets, each of said framed data packets containing an information portion;

detecting, on said communication device, a beginning of said information portion within one of said framed data packets; and

determining, on said communication device, whether said information portion contains said configuration information of a predetermined type,

wherein said communication device unframes said one of said framed data packets when said information portion contains said configuration information of a predetermined type.

2. The method of Claim 1, wherein said detecting includes scanning said plurality of said framed data packets and establishing said beginning of said information portion for one of said framed data packets by identifying a frame-demarcating character.

3. The method of Claim 2, wherein said detecting includes,

unescaping, on said communication device, contents of a predetermined number of bytes within said information portion, and

determining, on said communication device, whether said contents of said unescaped predetermined number of bytes includes predetermined characters,

wherein said communication device unescapes contents of additional consecutive bytes, succeeding said predetermined number of bytes, when said contents of said unescaped predetermined number of bytes includes said predetermined characters, and

wherein said communication device determines whether contents of said unescaped predetermined number of bytes and contents of additional

consecutive bytes contain said configuration information of a predetermined type.

4. The method of Claim 2, wherein said detecting includes,

determining, on said communication device, whether contents of a particular byte or bytes of said information portion contains information of a type associated with said particular byte, and

determining, on said communication device, whether said contents of said particular byte contains said configuration information of a predetermined type,

wherein said communication device progresses to a subsequent stage when said contents of said particular byte lacks said configuration information of a predetermined type and said configuration information of a predetermined type is disposed in a byte position subsequent to said particular byte.

5. The method of Claim 4, wherein said progresses to a subsequent stage further includes,

examining, on said communications device, contents of at least one succeeding byte of said information portion, said succeeding byte being subsequent to said particular byte, and

determining, on said communication device, whether contents of said succeeding byte contains information of a type associated with said succeeding byte, and

determining, on said communication device, whether said contents of said succeeding byte contains said configuration information of a predetermined type,

wherein said communication device sequentially examines successive bytes of said information portion until contents of said succeeding byte contains said configuration information of a predetermined type.

6. The method of Claim 5, wherein said contents of said particular byte and said contents of said succeeding byte includes escaped information.

7. The method of Claim 5, wherein said contents of said particular byte and said contents of said succeeding byte includes unescaped information.

8. A system for early detection of configuration information of a predetermined type, said system comprising:

a terminal device for transmitting and receiving a plurality of framed data packets, each of said framed data packets containing an information portion; and

a communication device coupled to said terminal device,

wherein said communication device detects a beginning of said information portion within one of said framed data packets and determines whether said information portion contains said configuration information of a predetermined type, and

wherein said communication device unframes said one of said framed data packets when said information portion contains said configuration information of a predetermined type.

9. The system of Claim 8, wherein said detecting by said communication device includes scanning said plurality of said framed data packets and establishing said beginning of said information portion for one of said framed data packets by identifying a frame-demarcating character.

10. The system of Claim 9, wherein said detecting by said communication device includes,

unescaping contents of a predetermined number of bytes within said information portion, and

determining whether said contents of said unescaped predetermined number of bytes includes predetermined characters,

wherein said communication device unescapes contents of additional consecutive bytes, succeeding said predetermined number of bytes, when said contents of said unescaped predetermined number of bytes includes said predetermined characters, and

wherein said communication device determines whether contents of said unescaped predetermined number of bytes and contents of additional consecutive bytes contain said configuration information of a predetermined type.

11. The system of Claim 9, wherein said detecting by said communication device includes,

determining whether contents of a particular byte or bytes of said information portion contains information of a type associated with said particular byte or bytes, and

determining whether said contents of said particular byte or bytes contains said configuration information of a predetermined type,

wherein said communication device progresses to a subsequent stage when said contents of said particular byte or bytes lacks said configuration information of a predetermined type and said configuration information of a predetermined type is disposed in a byte position subsequent to said particular byte or bytes.

12. The system of Claim 11, wherein said communication device progressing to a subsequent stage further includes,

examining contents of at least one succeeding byte of said information portion, said succeeding byte being subsequent to said particular byte, and

determining whether contents of said succeeding byte contains information of a type associated with said succeeding byte and whether said contents of said succeeding byte contains said configuration information of a predetermined type,

wherein said communication device sequentially examines successive bytes of said information portion until contents of said

succeeding byte contains said configuration information of a predetermined
12 type.

13. The method of Claim 12, wherein said contents of said
2 particular byte and said contents of said succeeding byte includes escaped information.

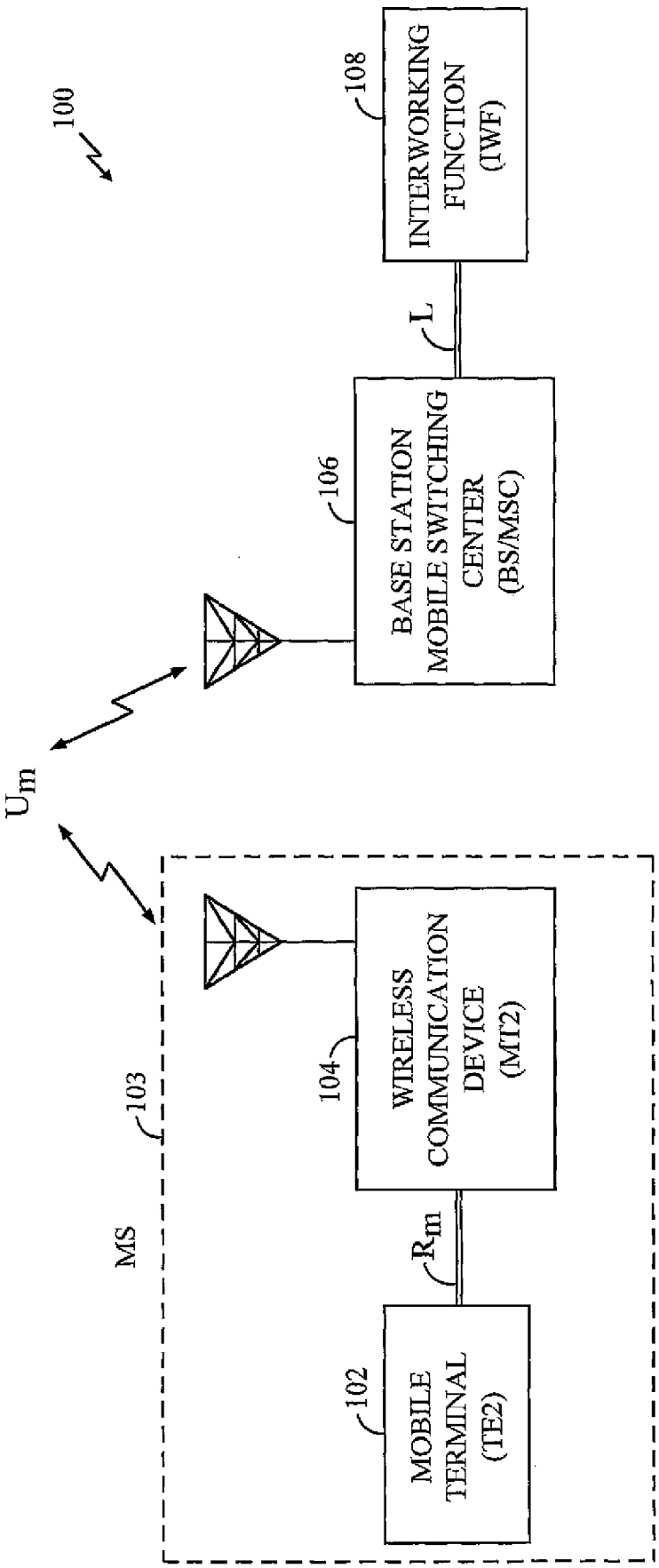

100
108
INTERWORKING FUNCTION (IWF)
L
106
BASE STATION MOBILE SWITCHING CENTER (BS/MSC)
U_m
MS
103
104
WIRELESS COMMUNICATION DEVICE (MT2)
R_m
102
MOBILE TERMINAL (TE2)

FIG. 1

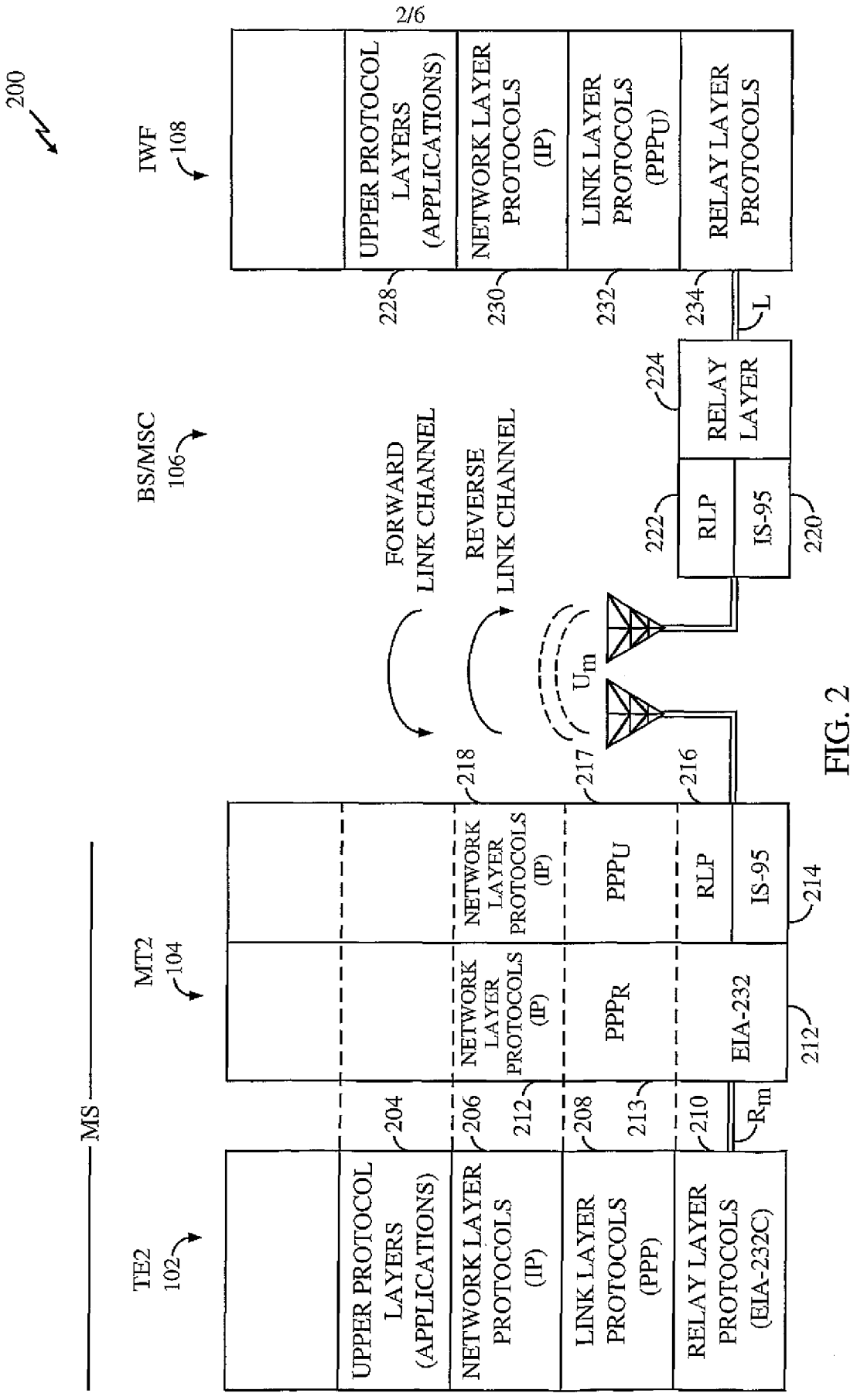

200
IWF
108
UPPER PROTOCOL LAYERS (APPLICATIONS)
NETWORK LAYER PROTOCOLS (IP)
LINK LAYER PROTOCOLS (PPPU)
RELAY LAYER PROTOCOLS
228
230
232
234
L
BS/MSC
106
FORWARD LINK CHANNEL
REVERSE LINK CHANNEL
224
RELAY LAYER
222
RLP
IS-95
220
Um
MS
MT2
104
NETWORK LAYER PROTOCOLS (IP)
PPPU
RLP
IS-95
214
218
217
216
NETWORK LAYER PROTOCOLS (IP)
PPPR
EIA-232
212
TE2
102
UPPER PROTOCOL LAYERS (APPLICATIONS)
NETWORK LAYER PROTOCOLS (IP)
LINK LAYER PROTOCOLS (PPP)
RELAY LAYER PROTOCOLS (EIA-232C)
204
206
212
208
213
210
Rm

FIG. 2

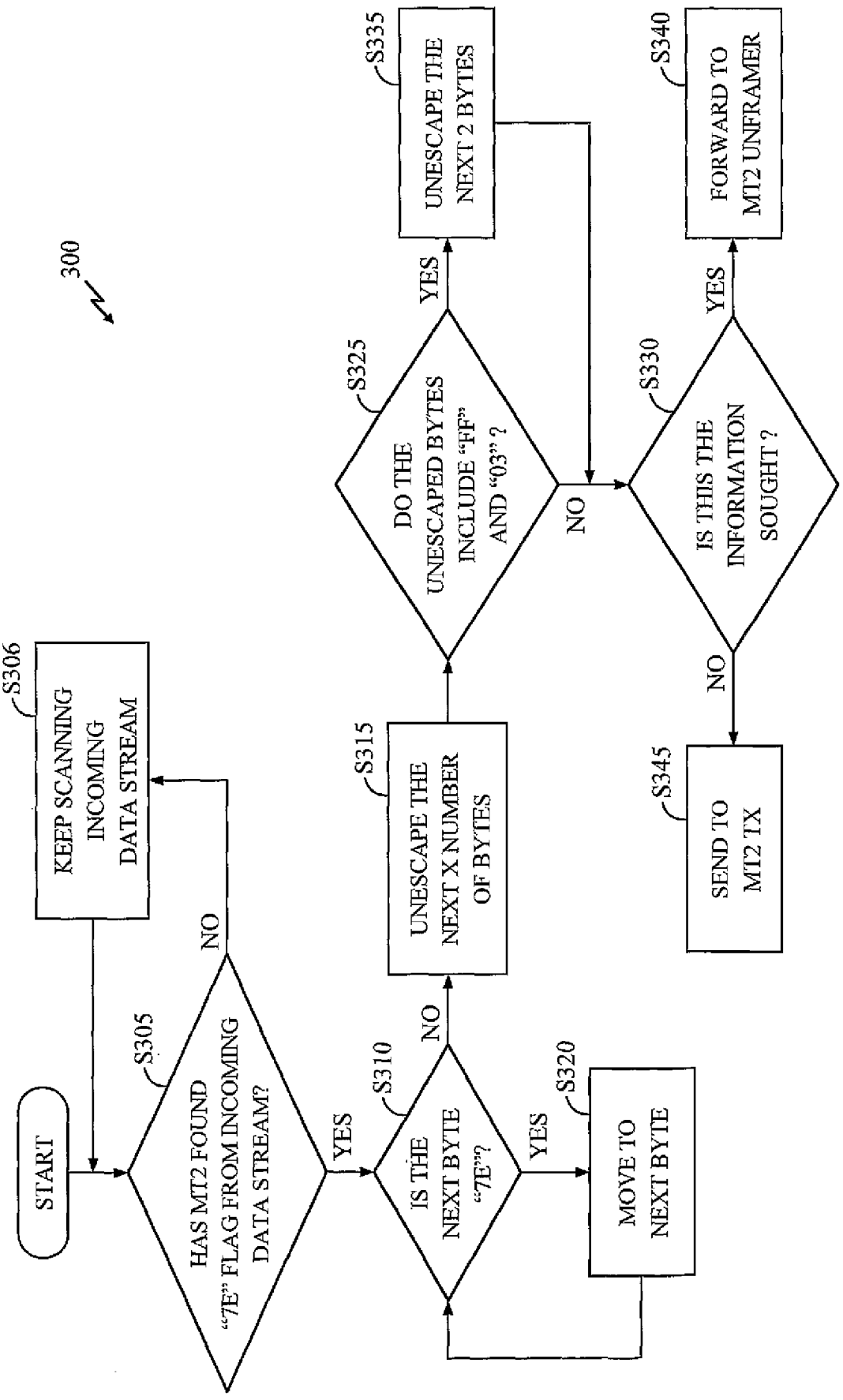

300
START
S305
HAS MT2 FOUND "7E" FLAG FROM INCOMING DATA STREAM?
NO
YES
S306
KEEP SCANNING INCOMING DATA STREAM
S310
IS THE NEXT BYTE "7E"?
NO
YES
S315
UNESCAPE THE NEXT X NUMBER OF BYTES
S320
MOVE TO NEXT BYTE
S325
DO THE UNESCAPED BYTES INCLUDE "FF" AND "03" ?
YES
NO
S330
IS THIS THE INFORMATION SOUGHT ?
YES
NO
S335
UNESCAPE THE NEXT 2 BYTES
S340
FORWARD TO MT2 UNFRAMER
S345
SEND TO MT2 TX

FIG. 3

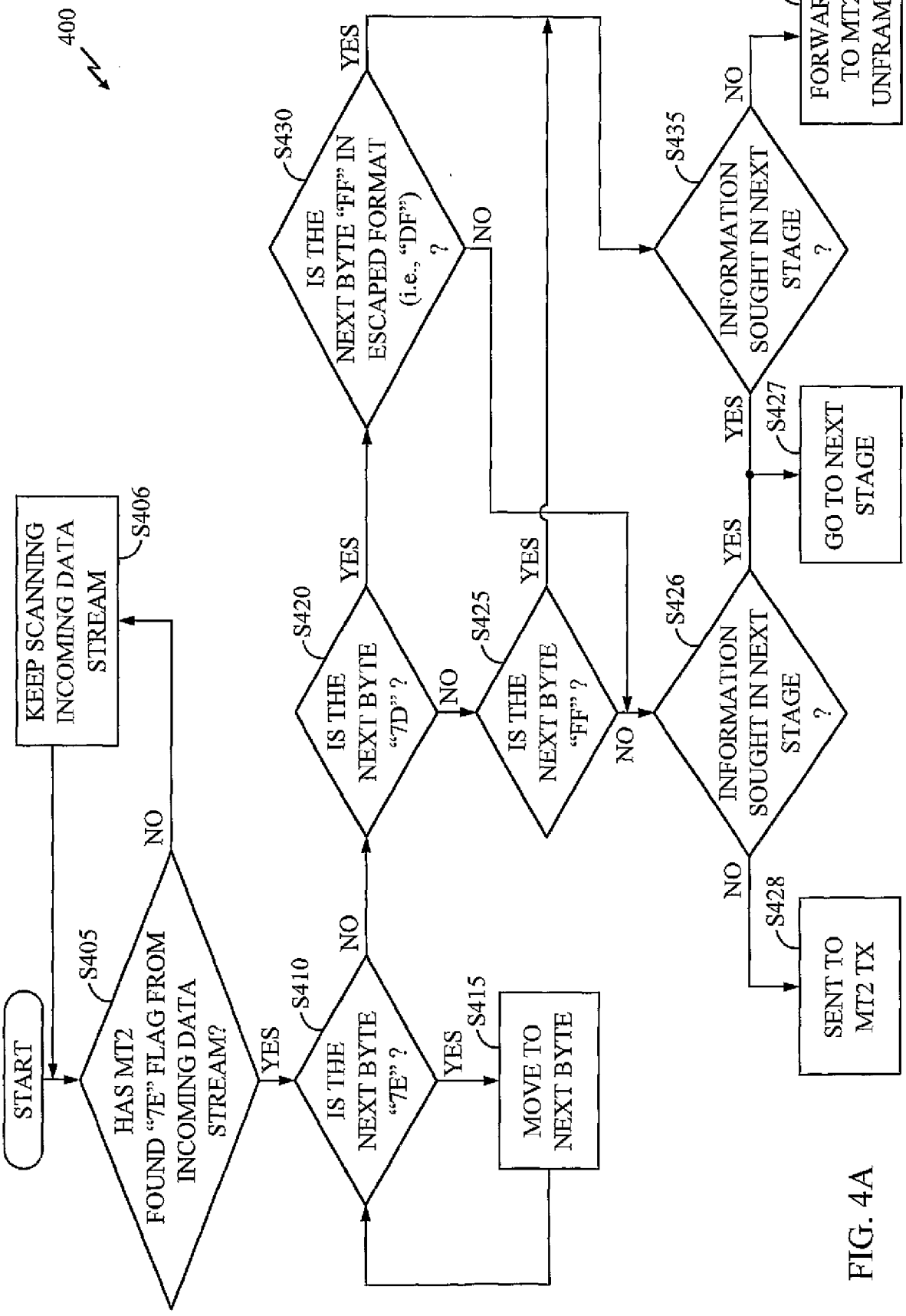

400
START
KEEP SCANNING INCOMING DATA STREAM
S406
S405
HAS MT2 FOUND "7E" FLAG FROM INCOMING DATA STREAM?
NO
YES
S410
IS THE NEXT BYTE "7E" ?
NO
YES
S415
MOVE TO NEXT BYTE
S420
IS THE NEXT BYTE "7D" ?
NO
YES
S425
IS THE NEXT BYTE "FF" ?
NO
YES
S430
IS THE NEXT BYTE "FF" IN ESCAPED FORMAT (i.e., "DF") ?
NO
YES
S426
INFORMATION SOUGHT IN NEXT STAGE ?
NO
YES
S428
SENT TO MT2 TX
S427
GO TO NEXT STAGE
S435
INFORMATION SOUGHT IN NEXT STAGE ?
NO
YES
S437
FORWARD TO MT2 UNFRAMER

FIG. 4A

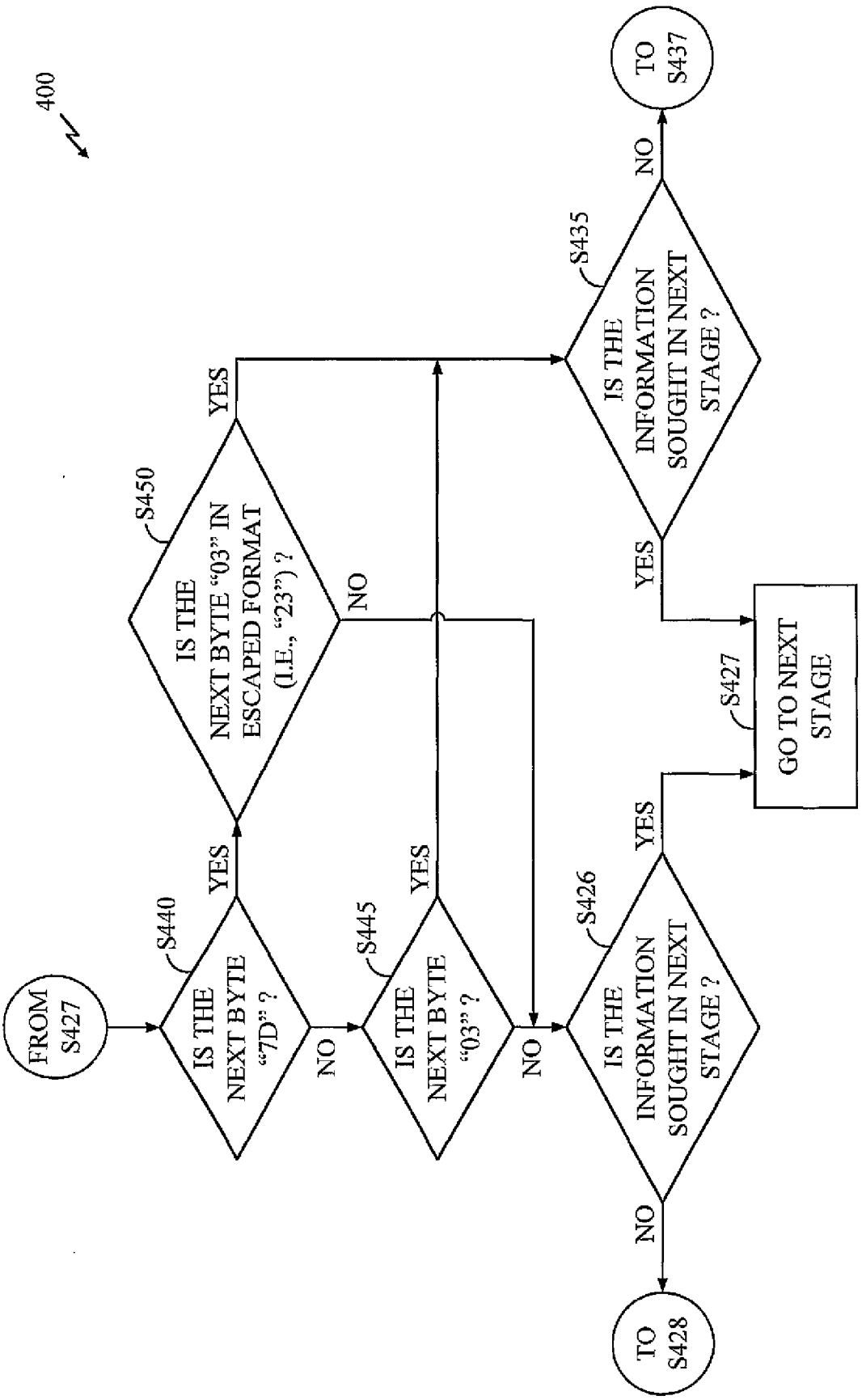

400
FROM S427
S440
IS THE NEXT BYTE "7D" ?
YES
NO
S445
IS THE NEXT BYTE "03" ?
YES
NO
S426
IS THE INFORMATION SOUGHT IN NEXT STAGE ?
YES
NO
TO S428
S450
IS THE NEXT BYTE "03" IN ESCAPED FORMAT (I.E., "23") ?
YES
NO
S435
IS THE INFORMATION SOUGHT IN NEXT STAGE ?
YES
NO
TO S437
S427
GO TO NEXT STAGE

FIG. 4B

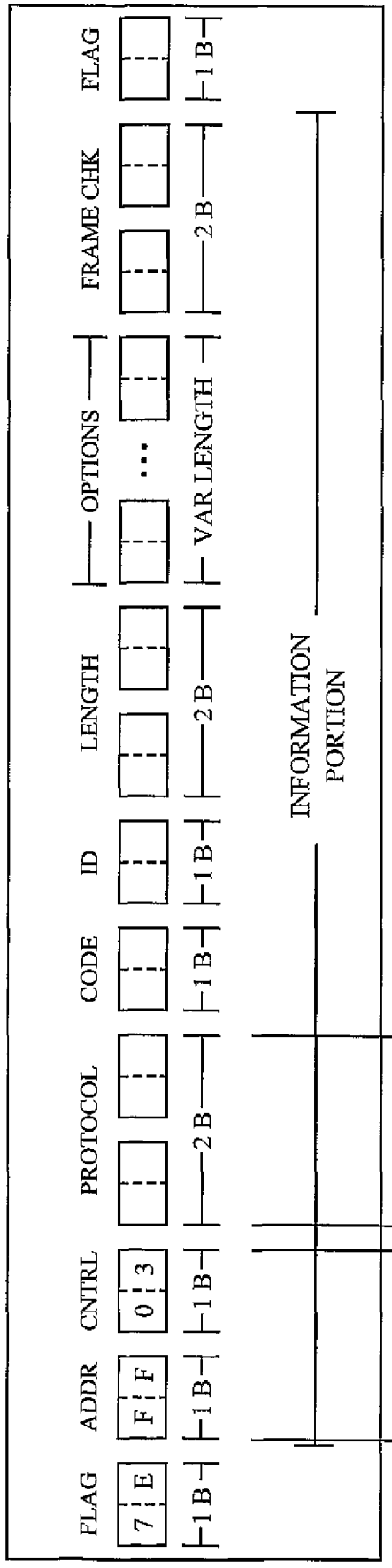

FLAG
ADDR
CNTRL
PROTOCOL
CODE
ID
LENGTH
OPTIONS
FRAME CHK
FLAG
7 E
F F
0 3
1 B
2 B
VAR LENGTH
INFORMATION PORTION
MAY BE COMPRESSED OUT
MAY BE COMPRESSED TO 1 BYTE

FIG. 5

INTERNATIONAL SEARCH REPORT

Interna Application No
PCT/US 00/24623

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/22 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 917 318 A (LUCENT) 19 May 1999 (1999-05-19) page 5, line 3 -page 33, line 39; figures	1-13
A	WO 96 21984 A (NOKIA) 18 July 1996 (1996-07-18) page 8, line 18 -page 17, line 22; figures	1,8
P,Y	WO 99 65178 A (ERICSSON) 16 December 1999 (1999-12-16) page 3, line 23 -page 9, line 12; figures	1,8
P,Y	WO 99 65219 A (IREADY) 16 December 1999 (1999-12-16) page 7, line 23 -page 26, line 13; figures	1,8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 July 2001	11/07/2001

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,
Fax: (+31–70) 340–3016

Authorized officer
Geoghegan, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No
PCT/US 00/24623

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 917318 A	19-05-1999	CA 2249817 A	14-04-1999
		CA 2249830 A	14-04-1999
		CA 2249831 A	14-04-1999
		CA 2249836 A	14-04-1999
		CA 2249837 A	14-04-1999
		CA 2249838 A	14-04-1999
		CA 2249839 A	14-04-1999
		CA 2249862 A	14-04-1999
		CA 2249863 A	14-04-1999
		EP 0912026 A	28-04-1999
		EP 0910198 A	21-04-1999
		EP 0917320 A	19-05-1999
		EP 0912027 A	28-04-1999
		EP 0912012 A	28-04-1999
		EP 0917328 A	19-05-1999
		EP 0918417 A	26-05-1999
		EP 0912017 A	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999
WO 9621984 A	18-07-1996	FI 950117 A	11-07-1996
		AU 699246 B	26-11-1998
		AU 4392996 A	31-07-1996
		CA 2209944 A	18-07-1996
		EP 0804845 A	05-11-1997
		JP 10512120 T	17-11-1998
		NO 973176 A	09-09-1997
		US 5978386 A	02-11-1999
WO 9965178 A	16-12-1999	AU 4667599 A	30-12-1999
WO 9965219 A	16-12-1999	AU 4435999 A	30-12-1999
		EP 1086573 A	28-03-2001

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年8 月8 日 (08.08.2002)

PCT

(10) 国際公開番号
WO 02/061572 A1

(51) 国際特許分類[7]: G06F 9/06, 9/445

(21) 国際出願番号: PCT/JP02/00699

(22) 国際出願日: 2002 年1 月30 日 (30.01.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-24738 2001 年1 月31 日 (31.01.2001) JP
特願2001-83567 2001 年3 月22 日 (22.03.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 夏野 剛 (NATSUNO,Takeshi) [JP/JP]; 〒153-0062 東京都 目黒区 三田一丁目５-６-１００２ Tokyo (JP). 板垣 崇稔 (ITAGAKI,Takatoshi) [JP/JP]; 〒134-0084 東京都 江戸川区 東葛西五丁目１５−４−５０２ Tokyo (JP). 森口 敦 (MORIGUCHI,Atsushi) [JP/JP]; 〒113-0033 東京都 文京区 本郷一丁目３０−２９−５０１ Tokyo (JP).

(74) 代理人: 川崎 研二 (KAWASAKI,Kenji); 〒103-0027 東京都 中央区 日本橋一丁目２番１０号 東洋ビルディング ７階 朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, JP, KR, NO, NZ, PH, PL, SG, US.

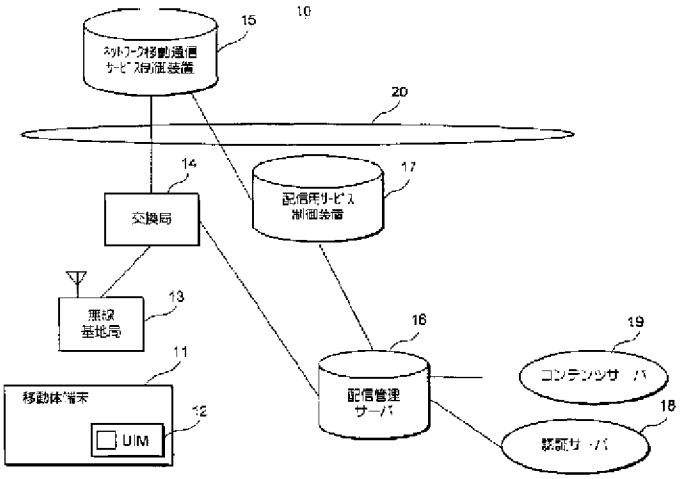
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: SYSTEM FOR DELIVERING PROGRAM TO STORAGE MODULE OF MOBILE TERMINAL

(54) 発明の名称: 移動体端末の記憶モジュールにプログラムを配信するシステム



15...NETWORK MOBILE COMMUNICATION SERVICE CONTROL APPARATUS
14...EXCHANGE
17...APPARATUS FOR CONTROLLING SERVICE TO BE DELIVERED
13...RADIO BASE STATION
11...MOBILE TERMINAL
16...DELIVERY MANAGING SERVER
19...CONTENT SERVER
18...AUTHENTICATION SERVER

(57) Abstract: A mobile terminal (11) has a built-in or mounted UIM (12) having a plurality of storage areas. Upon reception of a delivery request from the mobile terminal (11), a content server (19) delivers a program and data used when the program is executed or a single program unit via a network including a radio network. The program and the data or the single program unit are stored in a storage area of the UIM (12) without passing them through a control block of the mobile terminal (11).

(続葉有)

WO 02/061572 A1

(57) 要約:

移動体端末１１には、複数の記憶領域を有するＵＩＭ１２が内蔵あるいは装着されている。コンテンツサーバ１９は、この移動体端末１１からの配信要求を受けると、プログラムおよびこのプログラムの実行時に使用されるデータあるいはプログラム単体を無線ネットワークを含むネットワークを介して配信する。このプログラムおよびデータあるいはプログラム単体は、移動体端末１１の制御部を経由することなく、ＵＩＭ１２の記憶領域に格納される。

明細書

移動体端末の記憶モジュールにプログラムを配信するシステム

技術分野

本発明は、移動体端末に内蔵あるいは装着された記憶モジュールにプログラム（アプリケーションあるいはアプレット）を配信する技術に関する。

背景技術

近年、プログラム（アプリケーションあるいはアプレット）の実行環境を有する移動体端末が開発されている。そして、この種の移動体端末の一例としてＪａｖａのバーチャルマシンを搭載したものがある。ユーザは、移動体端末に外部からプログラムをインストールすることにより、所望の機能を移動体端末に追加することができる。

しかし、いくら所望の機能を追加したとしても、同じ移動体端末を継続して使っていればそのうち飽きてくるものである。一方、移動体端末の業界は競争が激しく、ユーザにとって魅力的な新製品が続々と提供されている。ユーザとしては、自分の気に入った製品が販売されたときには、現在のものから新製品に移動体端末に交換したいところである。ところが、移動体端末の交換を行ったとすると、折角それまでの移動体端末に追加した機能をもはや利用することができなくなってしまう。交換後も、これらの機能を利用するためには、古い移動体端末にインストールしたプログラムを新規な移動体端末にインストールしなければならない。これは面倒である。

発明の開示

この発明は以上のような事情に鑑みてなされたものであり、その目的は、移動体端末の交換が行われた場合でも、その交換前において使用可能であったプログラムを交換後においても継続して使用可能にすることにある。

この目的を達成するために、本願発明者らは、ある種の移動体端末に着目した。すなわち、加入者番号やメモリダイヤル情報等の加入者情報を記憶するモジュール（ユーザ識別モジュール；以下、ＵＩＭと略称する）の装着あるいは内蔵が可能な移動体端末である。この種の移動体端末のユーザは、移動体端末を新規なものに交換したいとき、自分自身の加入者情報が記憶されたＵＩＭを所持していれば、これを新規な移動体端末に装着しまたは内蔵させるだけで、その移動体端末を使用することができる。そして、本願発明者らは、次のような着想に至った。すなわち、このＵＩＭにプログラムを記憶させるようにすれば、移動体端末の交換時においても、交換前の移動体端末で利用していたプログラムを容易に新たな移動体端末に移行させることができ、ユーザの使い勝手が向上する、との着想である。

しかしながら、この着想を新規な移動体端末の実現に結び着けるにはセキュリティ上の問題があった。

まず、ＵＩＭへのプログラムの書き込みに何ら制限を設けないとすれば、故意または過失により移動体端末の本来の機能を損なうことが考えられ、好ましくない。

また、ＵＩＭに記憶される加入者情報には金銭的な価値を有するデータや個人情報が含まれている場合がある。従って、ＵＩＭへのプログラムの書き込みをセキュリティ確保の観点からもこれらの情報の漏洩など招かないような配慮が必要である。

このようなセキュリティ上の問題を解決し、ユーザの使い勝手を向上するために、本発明は、プログラムの配信要求を送信する手段を有する移動体端末と、前記移動体端末に内蔵あるいは接続された記憶モジュールと、前記配信要求を受信し、配信対象であるプログラムを送信するコンテンツサーバと、前記コンテンツサーバから前記プログラムを受信し、前記コンテンツサーバが予め許可されたコンテンツサーバである場合に限り、前記コンテンツサーバから受信したプログラムを前記移動体端末に内蔵あるいは接続された記憶モジュールに送信する配信管理サーバとを具備し、前記記憶モジュールは、記憶部と、前記移動体端末を介し

て前記配信管理サーバから受信されたプログラムを前記記憶部に記憶し、要求に応じて、前記記憶部に記憶されたプログラムを実行する制御部とを具備することを特徴とするプログラム配信システムを提供する。

また、本発明は、プログラムの配信要求を送信する手段を有する移動体端末と、前記移動体端末に内蔵あるいは接続された記憶モジュールと、前記配信要求を受信し、配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムである場合に、該プログラムを取得して前記移動体端末に内蔵あるいは接続された記憶モジュール宛てに送信する配信管理サーバとを具備し、前記記憶モジュールは、記憶部と、前記移動体端末を介して情報を受信し、該情報が前記配信管理サーバから受信されたプログラムである場合に限って前記記憶部に記憶し、要求に応じて、前記記憶部に記憶されたプログラムを実行する制御部とを具備することを特徴とするプログラム配信システムを提供する。

これらのシステムによれば、配信管理サーバを経由して、予め許可されたコンテンツサーバから供給されるプログラムのみが記憶モジュールに書き込まれるので、ユーザは、セキュリティを保証された状態で、新規なプログラムを記憶モジュールに書き込むことができる。

図面の簡単な説明

図１はこの発明の第１実施形態によるプログラム配信システムの構成を示すブロック図である。

図２は同実施形態における移動体端末の外観図である。

図３は同移動体端末の構成を示すブロック図である。

図４は同移動体端末およびこれに内蔵あるいは装着されたＵＩＭの構成を示す図である。

図５は同実施形態におけるプログラム配信からアクティベーションまでの過程を示すシーケンス図である。

図６は同実施形態におけるプログラム配信の動作を示すシーケンス図である。

図７はプログラム配信時における移動体端末の表示画面を示す図である。

図８は同実施形態におけるプログラムアクティベーションの動作を示すシーケンス図である。

図９は同実施形態においてコンテンツサーバからの要求によってプログラムディアクティベーションが行われる過程を示すシーケンス図である。

図１０は同実施形態においてコンテンツサーバからの要求によりプログラム削除が行われる過程を示すシーケンス図である。

図１１は同実施形態において配信管理サーバからの要求によりプログラムディアクティベーションおよびプログラム削除が行われる過程を示すシーケンス図である。

図１２は同実施形態において行われるＵＩＭのバージョン情報の授受を示すシーケンス図である。

図１３は、メモリ不足によりプログラム配信が未遂に終わる過程を示すシーケンス図である。

図１４は、メモリエラーによりプログラム配信が未遂に終わる過程を示すシーケンス図である。

図１５は、プログラム削除時にユーザに提供される表示画面を示す図である。

図１６は、電子商取引の決済時にユーザに提供される表示画面を示す図である。

図１７は、通信販売での商品購入時にユーザに提供される表示画面を示す図である。

図１８は、プログラムの自動起動設定時の表示画面を示す図である。

図１９および図２０は、定期券使用時の表示画面を示す図である。

図２１は、この発明の第２実施形態に係るプログラム配信システムの構成を示すブロック図である。

図２２は、同実施形態におけるＵＩＭ内のメモリにおける構成を示す図である。

図２３は、同実施形態における配信管理サーバ１６Ａの構成を示すブロック図である。

図２４は、ユーザ情報格納部への登録処理を示すシーケンス図である。

図２５および図２６は、ユーザ情報格納部に登録されているプログラムをＵＩ

Ｍ１２の基本ブロックのいずれかに登録する動作を示すシーケンス図である。

図２７および図２８は、ユーザ情報格納部に登録されているプログラムをＵＩＭの基本ブロックのいずれかに登録する動作を示すシーケンス図である。

図２９は、ユーザ情報格納部５１に登録されているプログラムを削除する場合の動作を示すシーケンス図である。

図３０は、ＵＩＭの基本ブロックから登録されているプログラムを削除する動作を示すシーケンス図である。

図３１は、ユーザ情報格納部ディアクティベーション処理を示すシーケンス図である。

図３２は、基本ブロックディアクティベーション処理を示すシーケンス図である。

発明を実施するための最良の形態

次に本発明の好適な実施形態について、図面を参照して説明する。

［１］第１実施形態

［１．１］プログラム配信システムの概要構成

図１はこの発明の第１実施形態に係るプログラム配信システムの構成を示すブロック図である。

プログラム配信システム１０は、大別すると、移動体端末１１と、無線基地局１３と、交換局１４と、ネットワーク移動通信サービス制御装置１５と、配信管理サーバ１６と、配信用サービス制御装置１７と、認証サーバ１８と、コンテンツサーバ１９と、一般公衆回線ネットワーク２０とを備えている。

移動体端末１１は、例えば、携帯電話、ＰＨＳ（Personal Handyphone System；登録商標）等の通信機能を有する情報処理装置である。さらに移動体端末１１は、各種プログラムあるいはデータを記憶可能なＵＩＭ（User Identification Module）１２が装着あるいは内蔵されている。

無線基地局１３は、無線リンクを介して移動体端末１１と通信を行う。

交換局１４は、無線基地局１３を介して接続される移動体端末１１と有線ネッ

トワークである共通線信号方式ネットワーク２０との間で交換制御を行う。

ネットワーク移動通信サービス制御装置１５は、一般公衆回線ネットワーク２０を介して移動体端末１１に対してプログラム配信を行う場合に通信制御を行う。

コンテンツサーバ１９は、各種コンテンツを配信するとともに、移動体端末１１から要求されたプログラムの配信を行う。

配信管理サーバ１６は、コンテンツサーバ１９からＵＩＭ１２へのプログラムの配信の中継およびその管理を行う。ＵＩＭ１２へのプログラムの配信およびＵＩＭ１２に格納されたプログラムへのアクセスは、常にこの配信管理サーバ１６を経由して行われる。ここに本実施形態の最大の特徴がある。

配信用サービス制御装置１７は、一般公衆回線ネットワーク２０を介してプログラム配信を行う場合に配信管理サーバ１６と一般公衆回線ネットワーク２０との間のインターフェース的な動作を行う。

認証サーバ１８は、コンテンツサーバ１９にプログラムの配信に必要な証明書の発行を行う装置である。この証明書には、コンテンツサーバ１９がＵＩＭ１２にプログラムを配信する正当権限を有する者であることをＵＩＭ１２のための証明する役割を持ったＵＩＭ公開鍵と、コンテンツサーバ１９が同正当権限を持った者であることを配信管理サーバ１６のための証明する役割を持った配信管理サーバ公開鍵とがある。

本実施形態におけるコンテンツサーバ１９、配信管理サーバ１６および認証サーバ１８の役割分担は次の通りである。

ａ．本実施形態では、コンテンツサーバ１９は、ＵＩＭ１２宛のプログラムを配信管理サーバ１６に送り、この配信管理サーバ１６がＵＩＭ１２へのプログラムの配信を行う。コンツサーバ１９が、直接、ＵＩＭ１２にプログラムを配信することはない。

ｂ．コンテンツサーバ１９は、配信管理サーバ１６によって中継されつつ、公開鍵方式の暗号化通信によりＵＩＭ１２にプログラムを配信する。個々のユーザのＵＩＭ１２には、予めＰＫＩ（Public Key Infrastructure）が実装されており、ＵＩＭ１２は当該ＵＩＭ１２に固有のＵＩＭ秘密鍵を有している。コンテンツサ

ーバ１９は、あるＵＩＭ１２宛のプログラム配信を行うとき、そのＵＩＭ１２のＵＩＭ秘密鍵と対をなすＵＩＭ公開鍵を認証サーバ１８から取得し、これによってプログラムを暗号化する。

ｃ．本実施形態では、予め許可されたコンテンツサーバ１９のみがＵＩＭ１２宛のプログラムの配信を行うことができる。許可されたコンテンツサーバ１９には配信管理サーバ公開鍵が予め与えられる。コンテンツサーバ１９は、移動体端末１１からの配信要求があったとき、ＵＩＭ公開鍵によって暗号化されたＵＩＭ１２宛のプログラムを配信管理サーバ公開鍵によってさらに暗号化し、配信管理サーバ１６に送る。

［１．２］移動体端末の構成

図２に移動体端末１１の外観図を示す。

移動体端末１１は、ディスプレイ部２１と、操作部２２とを備えている。

ディスプレイ部２１には、図２に示すように、各種処理メニューやブラウジング中の画面、電話番号画面などが表示される。

操作部２２は、各種データの入力や、メニュー画面の表示を行わせるための複数の操作ボタンが設けられている。この操作部２３の操作ボタンの一つとしてＵＩＭボタン２３がある。このＵＩＭボタン２３は、ユーザがＵＩＭ１２に記憶されたプログラムを利用する際に操作するボタンである。

図３は移動体端末の構成を示すブロック図である。

移動体端末１１は、ディスプレイ部２１と、操作部２２と、制御部３１と、記憶部３２と、外部機器インターフェース（Ｉ／Ｆ）部３３と、通信部３４と、ＵＩＭインターフェース（Ｉ／Ｆ）部３５と、音声入出力部３６とを備えている。

制御部３１は、記憶部３２に記憶されている制御プログラム、制御データに基づいて移動体端末１１の各部を制御する。

記憶部３２は、ＲＯＭ、ＲＡＭ等から構成されており、インターネットにアクセスするためのブラウザなどの各種プログラムを記憶するプログラム記憶領域や各種データを記憶するデータ記憶領域等、複数の記憶領域を有している。

外部機器Ｉ／Ｆ部３３は、制御部３１やＵＩＭ１２が外部の装置との間で情報

の授受を行う際に利用されるインタフェースである。

通信部３４は、制御部３１による制御の下、アンテナ３４Ａを介して音声、文字メッセージ等各種データを無線基地局１３に送信する一方、アンテナ３４Ａを介して移動体端末１１宛に送られてくる各種データを受信する。

ＵＩＭＩ／Ｆ部３５は、制御部３１との間でデータの入出力を行う。また、ＵＩＭＩ／Ｆ部３５は、通信部３４あるいは外部機器Ｉ／Ｆ部３３のいずれかからの出力データを制御部３１を介さずにＵＩＭ１２に出力する。また、ＵＩＭ１２の出力データを制御部３１を介さずに、外部機器Ｉ／Ｆ部３３あるいは通信部３４のいずれかに直接出力する。このように制御部３１を介さずに外部機器Ｉ／Ｆ部３３あるいは通信部３４との間でデータの入出力を行わせるのは、制御部３１の制御プログラムの改竄などによってＵＩＭ１２上のデータへの不正なアクセスが行われるのを防止し、セキュリティを確保するためである。

［１．３］ＵＩＭの構成

図４にＵＩＭ１２の構成を示す。なお、図４には移動体端末１１との関係を明らかにするため、ＵＩＭ１２の構成要素とともに移動体端末１１の構成要素の一部が示されている。図４に示すように、ＵＩＭ１２は、メモリ１２Ｍを有しており、このメモリ１２Ｍは、大別すると、システム領域１２Ａと、アプリケーション領域１２Ｂとを備えている。

システム領域１２Ａは、加入者番号データ、発信履歴情報データ、着信履歴情報データ、通話時間情報データ、ＵＩＭ秘密鍵といったユーザ固有の個人情報データが格納されている。移動体端末１１は、このシステム領域１２Ａ内の加入者番号データを発番号として利用し、他の通信装置との通信を行う。

アプリケーション領域１２Ｂは、配信されたプログラムおよびこのプログラムの実行時に使用されるデータを記憶する領域であり、複数の基本ブロックに分けられている。図４に示す例では、アプリケーション領域１２Ｂは、６個の基本ブロック４０－１～４０－６に分けられている。

各基本ブロック４０－１～４０－６は、それぞれプログラム領域４１およびデータ領域４２を備えている。各基本ブロック４０－ｋのプログラム領域４１は、

プログラム（アプリケーションあるいはアプレット）が格納される。また、各基本ブロック４０－ｋのデータ領域４２は、同一基本ブロック４０－ｋにおけるプログラム領域４１内のプログラムの実行時に使用されるデータが格納される。

基本ブロック４０－１～４０－６は、互いに独立しており、原則的には、ある基本ブロック４０－ｊのプログラム領域４１に格納されたアプリケーションあるいはアプレットが他の基本ブロック４０－ｋ（≠ｊ）のデータ領域４２にアクセスすることはできないように管理されている。このような構成を採ることにより各プログラムのセキュリティを確保しているのである。従って、ある基本ブロック４０－ｊのデータ領域４２に金銭的な価値を有するデータ（いわゆる、バリュー；value）を記録しておいたとしても、このデータが他の基本ブロック４０－ｋ（≠ｊ）に格納されているプログラムにより故意または偶然に書き換えられることはない。

また、プログラム領域４１に格納されたプログラムであるアプリケーションあるいはアプレットについては、配信管理サーバ１６を経由しないかぎり配信、削除などを行うことはできない。ただし、データ領域４２については、ＡＴＭから電子マネーをダウンする場合のように、配信管理サーバ１６経由あるいはローカルな端末を介して直接操作することが可能となっている。

さらにアプリケーション領域１２には、各基本ブロック４０－１～４０－６に対応して、各基本ブロックのプログラム領域４１内のプログラムが実行可能であるか否かを示す活性化フラグの記憶領域が設けられている。

制御部３０は、移動体端末１１を介して与えられる要求に応じて、アプリケーション領域１２Ｂの基本ブロックに対するプログラムの書き込みを行ったり、各基本ブロックに対応した活性化フラグのセットまたはリセットを行ったり、指定された基本ブロック内のプログラムを実行する手段である。配信管理サーバ１６からＵＩＭ公開鍵によって暗号化されたプログラムが届いたとき、制御部３０はシステム領域１２Ａ内のＵＩＭ秘密鍵を用いてプログラムを復号化を行い、いずれかの基本ブロックに書き込む。また、制御部３０は、基本ブロック内のプログラムを実行することができ、その際に、移動体端末１１側において実行されるプ

ラウザを介して、実行中のプログラムが必要とする情報をネットワーク内の通信相手から取得したり、移動体端末１１のユーザから取得する。制御部３０は、逆に、ブラウザを介して、プログラムの実行結果をネットワーク内の通信相手に送ったり、移動体端末１１のユーザに送ることもできる。また、制御部３０は、基本ブロック内のプログラムに従って、ブラウザを介することなく、移動体端末１１のハードウェア資源を介して外部との授受を行うことができる。例えばこの種のプログラムとして移動体端末１１を定期券として機能させるアプリケーションプログラムがある。かかるプログラムを実行する場合、制御部３０は、移動体端末３０の外部機器Ｉ／Ｆに接続された近距離無線装置（図示略）を利用して、駅の改札口のカードリーダ／ライタと、定期券情報の授受を行うことができる。制御部３０がアプリケーション領域内のプログラムの実行制御を含む以上のような各種の処理を行うためのプログラムは、システム領域１２Ａに格納されている。

［１．４］第１実施形態の動作

次に定期券用アプレットの配信を例として第１実施形態の動作を説明する。

図５はプログラム配信、書き込みおよび活性化の過程を示すシーケンス図である。

図５に示すように、これらの一連の処理は、大別すると、不活性状態のプログラム（アプレット）を記憶モジュールとしてのＵＩＭ１２に配信して、書き込む処理（ステップＳ１）と、書き込んだプログラムを活性化するアクティベーション処理（ステップＳ２）とにより構成されている。

［１．４．１］配信管理サーバに対する証明書発行

図６はプログラム配信およびＵＩＭ１２への書き込みの過程を示すシーケンス図である。図６に示すように、認証サーバ１８は、ＵＩＭ１２宛てのプログラム配信を許可したコンテンツサーバ１９に対して証明書を発行する（ステップＳ１１）。この証明書の発行は、コンテンツサーバ１９と配信管理サーバ１６とが公開鍵暗号化方式による暗号化通信を行うために行われるものである。すなわち、公開鍵暗号化方式による暗号化通信を可能にするため、対をなす配信管理サーバ秘密鍵と配信管理サーバ公開鍵が生成され、配信管理サーバ秘密鍵は配信管理サ

ーバ１６に記憶され、配信管理サーバ公開鍵は、プログラム配信を許可された者であることを証する証明書として認証サーバ１８からコンテンツサーバ１９に送信されるのである。コンテンツサーバ１９は、この配信管理サーバ公開鍵を受信すると、これをプログラムの配信に備えて保存する。

［１．４．２］プログラム配信要求

ユーザは、移動体端末１１の操作部２２を操作することにより、制御部３１にブラウザを実行させ、コンテンツプロバイダのホームページにアクセスすることができる。このアクセスにより、移動体端末１１のディスプレイ部２１には、図７に示すように、コンテンツプロバイダのコンテンツサーバ１９によって行われるプログラムの配信を表す配信メニュー画面Ｄ１が表示される。ユーザは、この状態において、移動体端末１１の操作部２２を操作することにより、プログラム（アプレット）配信要求を移動体端末１１からネットワークを介してコンテンツサーバ１９に送信することができる（ステップＳ１２）。

［１．４．３］ＵＩＭに対する証明書要求

コンテンツサーバ１９は、移動体端末１１から配信要求を受信すると、証明書発行要求を認証サーバ１８に送る（ステップＳ１２）。この証明書発行要求には移動体端末１１のＵＩＭ１２を特定する情報が含まれている。ここで、証明書の発行は、コンテンツサーバ１９がＵＩＭ１２と公開鍵方式の暗号化通信を行うために要求されるものである。さらに詳述すると、公開鍵方式の暗号化通信を可能にするため、対をなすＵＩＭ秘密鍵とＵＩＭ公開鍵が予め生成され、ＵＩＭ秘密鍵はＵＩＭ１２に予め格納され、ＵＩＭ公開鍵は認証サーバ１８に予め格納される。ステップＳ１２では、この認証サーバ１８に格納されたＵＩＭ公開鍵が、ＵＩＭ１２宛てのプログラム配信が許可された者であることを証する証明書として要求されるのである。

［１．４．４］証明書の発行およびＵＩＭに対する証明書付きプログラムの配信

認証サーバ１８は、コンテンツサーバ１９から証明書の発行要求を受信すると、この発行要求により特定されたＵＩＭ１２に対応するＵＩＭ公開鍵を証明書として、コンテンツサーバ１９に対して発行する（ステップＳ１４）。

コンテンツサーバ１９は、ＵＩＭ１２に対応するＵＩＭ公開鍵を用いて、配信要求のあったプログラムを暗号化する。この暗号化により得られたプログラムは、ＵＩＭ１２に対するアクセス権限を持った正当者であることを証する証明書が添付されたプログラムであるといえる。

次にコンテンツサーバ１９は、ＵＩＭ公開鍵によって暗号化されたプログラムを、事前に認証サーバ１８から受け取った配信管理サーバ公開鍵によりさらに暗号化する。この暗号化により得られたプログラムは、ＵＩＭ１２に対するアクセス権限を持った正当者であることを証する証明書と配信管理サーバ１６経由でプログラム配信を行うことができる正当者であることを証する証明書の両方が添付されたプログラムであるということができる。

［１．４．５］プログラム配信

コンテンツサーバ１９は、以上の２度に亙る暗号化を経て得られたプログラムをネットワークを介して配信管理サーバ１６に配信する（ステップＳ１５）。

配信管理サーバ１６は、配信管理サーバ秘密鍵を用いて、コンテンツサーバ１９から配信された暗号化プログラムを復号化する。この復号化が成功すると、ＵＩＭ公開鍵のみにより暗号化されたプログラムが得られる。この場合、コンテンツサーバ１９は、ＵＩＭ１２宛てのプログラム配信をする権限を有する正当者であるということができる。そこで、配信管理サーバ１６は、図７に示す画面Ｄ２のデータを移動体端末１１に送信し、ディスプレイ部２１に表示させる。この画面Ｄ２は、プログラム配信の可否をユーザに問い合わせる画面である。

［１．４．６］ＵＩＭ書込

ユーザが、画面Ｄ２を確認し、操作部２２を用いてプログラムの配信を許可する操作を行うと、配信許可の通知が配信管理サーバ１６に送られる。配信管理サーバ１６は、この通知を受け取ると、ＵＩＭ１２宛てに、上記復号化により得られたプログラム、すなわち、ＵＩＭ公開鍵によって暗号化されたプログラムを配信する（ステップＳ１６）。

この暗号化されたプログラムは移動体端末１１を介してそのままＵＩＭ１２の制御部３０に引き渡される。すなわち、移動体端末１１は、ＵＩＭ１２に対して

通信機能を提供するだけである。このような動作を移動体端末１１に行わせることにより、セキュアなＵＩＭ１２への伝送、書き込みを保証している。

ところで、以上のようにして配信管理サーバ１６がＵＩＭ１２にプログラムを送るためには、配信管理サーバ１６がＵＩＭ１２との間にリンクを確立する必要があり、そのためにはＵＩＭ１２が接続または内蔵されている移動体端末１１の電話番号を取得する必要がある。

そのための方法としては、移動体端末１１からコンテンツサーバ１９への配信要求の際に、移動体端末１１の電話番号をコンテンツサーバ１９に伝達させ、コンテンツサーバ１９がこの電話番号を配信管理サーバ１６に送る、という方法が考えられる。この場合、配信管理サーバ１６は、送られてきた電話番号を用いて移動体端末１１を呼び出し、ＵＩＭ１２宛てのプログラムを配信することができる。

また、別の方法として、次のものもある。すなわち、移動体端末１１からコンテンツサーバ１９への配信要求に先立って、移動体端末１１と配信管理サーバ１６との間で移動体端末１１の電話番号の代わりの識別子を取り決め、配信管理サーバ１６は電話番号と識別子とを対応付けて記憶する。そして、移動体端末１１は、コンテンツサーバ１９宛てに識別子を含んだ配信要求を送り、コンテンツサーバ１９はプログラムを配信管理サーバ１６に送るときに識別子を添付する。配信管理サーバ１６は、識別子から移動体端末１１の電話番号を求め、この電話番号により移動体端末１１を呼び出してＵＩＭ１２宛てのプログラムの配信を行う。この方法は、コンテンツサーバ１９に移動体端末１１の電話番号を知らせる必要がないという利点がある。

ＵＩＭ１２の制御部３０は、以上のようにしてＵＩＭ公開鍵によって暗号化されたプログラムを受け取ると、ＵＩＭ公開鍵と対をなすＵＩＭ秘密鍵を用いて、プログラムの復号化を行う。この復号化が成功すると、暗号化されていない平文のプログラムが得られる。この場合、送信元であるコンテンツサーバ１９は、ＵＩＭ１２へのプログラム配信をする正当な権限を有する者であるといえる。そこで、ＵＩＭ１２は、復号化により得られたプログラムをメモリの基本ブロック４

０－１～４０－６のいずれかに書き込む。

この書き込み中は、図７に示すような画面Ｄ３が移動体端末１１によって表示される。

［１．４．７］書込完了応答

ＵＩＭ１２の制御部３０は、プログラムの書き込みが終了すると、その旨をしめす書込完了通知を当該プログラムを書き込んだ基本ブロックを特定する情報とともに配信管理サーバ１６に対して送信する（ステップＳ１７）。

このとき、移動体端末１１のディスプレイ部２１には、図７に示すように、書き込みが終了した（登録が完了した）旨の画面Ｄ４が表示される。その後、ユーザの操作により画面は再び画面Ｄ１となる。

［１．４．８］配信完了通知

配信管理サーバ１６は、ＵＩＭ１２からプログラムの書込完了の通知を受けると、当該プログラムが書き込まれたＵＩＭ１２の基本ブロックを表す情報に対応づけて、書き込んだプログラムを特定する情報をデータベースに登録する。

配信管理サーバ１６は、このデータベースを参照することにより全てのＵＩＭ１２の基本ブロック４０－１～４０－６について各々に格納されているプログラムを容易に把握することができる。

配信管理サーバ１６は、ＵＩＭ１２内に対してプログラムを配信したとき、プログラムの配信元であるコンテンツサーバ１９のコンテンツプロバイダに対する課金処理を開始する。なお、課金処理の開始タイミングについては、これに限定されるものではなく、例えば、後述するアクティベーションが行われた段階で開始してもよい。

コンテンツプロバイダに対する課金対象として次の項目がある。

ａ．ＵＩＭ１２内の基本ブロックの貸与料金

コンテンツサーバ１９からのプログラムがＵＩＭ１２に配信されると、このプログラムは、ＵＩＭ１２内の基本ブロック４０－１～４０－６のうちのいずれかの基本ブロックに保存される。この場合の基本ブロックは、プログラムの保存のためにコンテンツサーバ１９を所有するコンテンツプロバイダに貸与されている

と考えることができる。そこで、この貸与されている期間、すなわち、プログラムが基本ブロックに保存されている期間に応じた料金を貸与料金としてコンテンツプロバイダから徴収するのである。

b．トランザクション料

コンテンツサーバ１９から送信されたプログラムは、配信管理サーバ１６の処理を経て、ＵＩＭ１２に配信される。この配信管理サーバ１６の処理に対する対価をトランザクション料としてコンテンツプロバイダから徴収するのである。

なお、ＵＩＭ１２のユーザは、コンテンツサーバ１９からプログラムの配信というサービスを受けているので、そのサービス利用料に関する課金の対象者となる。そこで、配信管理サーバ１６が、ユーザの通信料金とともにコンテンツプロバイパに代わってサービス利用料金をユーザから回収し、サービス利用料金をコンテンツプロバイダに引き渡すようにしてもよい。いわゆる代行回収である。この場合において、コンテンツプロバイダに課金される料金の中に、回収代行手数料を含めてもよい。

以上のようにしてプログラム配信が完了すると、配信管理サーバ１６は、その旨の通知をコンテンツサーバ１９に対して行う（ステップＳ１８）。

［１．４．９］アクティベーション

ＵＩＭ１２に配信され、基本ブロックに格納されたプログラムは、アクティベーション（活性化；Activation）が行われるまでは、ユーザが実行することはできない。

このように、プログラムを配信するだけでユーザに自由な実行を許可しないのは、プログラムの実行開始時期をコンテンツプロバイダなどが制御し得るようにするためである。

このアクティベーションが有効活用される場合として、例えば、新規発売するゲーム用プログラムのように、使用開始時期を限定する必要がある場合がある。この場合にアクティベーションを活用すると、発売開始日（プログラム配信日）と使用開始日（アクティベーション日）とを別個に設定可能となり、コンテンツサーバ１９の負荷を軽減することが可能となる。

また、別の例として、移動体端末１１を定期券として機能させるプログラムをＵＩＭ１２に配信する場合がある。この場合、定期券の有効期間の初日に、そのプログラムの実行可能状態にするためにアクティベーションが利用される。

以下、アクティベーション時の動作について図８を参照して説明する。

［１．４．９．１］配信管理サーバへのアクティベーション要求

コンテンツサーバ１９は、あるプログラムのアクティベーションが必要になったとき、配信管理サーバ１６に対してアクティベーション要求を送る（ステップＳ２１）。このアクティベーション要求は、アクティベーションの対象となるプログラムを特定する情報を含んでいる。また、特定のユーザのＵＩＭ１２に格納されたプログラムのみのアクティベーションを行うときには、そのユーザに対応した識別子（移動体端末１１の電話番号またはこれに代わる識別子）を含む。

［１．４．９．２］ＵＩＭへのアクティベーション要求

配信管理サーバ１６は、このアクティベーション要求を受け取ると、移動体端末１１のＵＩＭ１２に対して、アクティベーション要求を行う（ステップＳ２２）。既に述べたように、配信管理サーバ１６のデータベースには、プログラムが書き込まれたＵＩＭ１２の基本ブロックを表す情報に対応づけて、書き込んだプログラムを特定する情報が登録されている。配信管理サーバ１６は、アクティベーション要求を受け取ったとき、このデータベースを参照することにより、アクティベーションの対象であるプログラムが配信されたＵＩＭ１２と書き込み先である基本ブロックを求める。なお、複数のＵＩＭ１２に格納された同一プログラムのアクティベーションを行うときにはそのＵＩＭ１２の数だけこの処理が行われることになる。そして、該当するＵＩＭ１２が装着または内蔵された各移動体端末１１を呼び出し、ＵＩＭ１２宛てにアクティベーション要求を送る。各移動体端末１１に送られるアクティベーション要求は、アクティベーションの対象となるプログラムが格納された基本ブロックを特定する情報を含んでいる。

このアクティベーション要求は、移動体端末１１に受信されると、そのままＵＩＭ１２に送られる。ＵＩＭ１２の制御部３０は、アクティベーション要求に従ってアクティベーションを実行する。すなわち、ＵＩＭ１２は、アクティベーシ

ョン要求によって特定された基本ブロックについて、その活性化フラグを“０”から“１”に変更する。ＵＩＭ１２の制御部３０は、このようにして活性化フラグが“１”にされた基本ブロック内のプログラムの実行要求があったときはそれに応える。しかし、活性化フラグが“０”である基本ブロック内の実行要求があった場合にはその要求を拒否する。

［１．４．９．３］アクティベーション終了応答

ＵＩＭ１２は、プログラムのアクティベーションが終了すると、その旨をしめすアクティベーション終了通知を配信管理サーバ１６に対して送信する（ステップＳ２３）。この通知は、アクティベーションが終了したプログラムを特定する情報、より具体的にはそのプログラムが格納されている基本ブロックを特定する情報を含む。

［１．４．９．４］アクティベーション完了通知

配信管理サーバ１６は、ＵＩＭ１２からプログラムのアクティベーション完了の通知を受けると、これに基づいて、アクティベーションが完了したプログラムの格納先であるＵＩＭ１２の基本ブロックを求める。そして、その基本ブロックのために用意されたデータベース内の記憶領域にアクティベーションが完了した旨の情報を登録する。

この登録の結果、配信管理サーバ１６は、データベースを参照することにより全てのＵＩＭ１２について、各基本ブロック４０－１～４０－６内の各プログラムが活性化されているか否かを把握することができる。

アクティベーション要求のあったプログラムの全ての配信先ＵＩＭについてアクティベーション完了の登録を終えると、配信管理サーバ１６は、プログラムのアクティベーションが完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ２４）。この通知は、アクティベーションの対象となったプログラムを特定する情報を含んでいる。

［１．４．１０］ディアクティベーション

ＵＩＭ１２に配信され、活性化されたプログラムを不活性化（ディアクティベーション；Deactivation））することが必要となることがある。例えば、移動体

端末１１をクレジットカードとして機能させるプログラムがＵＩＭ１２に格納されており、そのＵＩＭ１２をユーザが紛失したような場合である。この場合、その紛失の事実を知ったユーザからの要請によりディアクティベーションが起動されることとなる。その他の例として、あるサービスを受けているユーザがそのサービス利用料を滞納しているような場合がある。この場合、そのようなサービスを提供しているコンテンツプロバイダからの要請により、そのサービスを受けるためのプログラムについてのディアクティベーションが起動されることになろう。

以下、ディアクティベーションについて図９を参照して説明する。

［１．４．１０．１］配信管理サーバへのディアクティベーション要求

コンテンツサーバ１９は、あるＵＩＭ１２に配信したプログラムについてディアクティベーションを行う必要が生じたとき、そのＵＩＭ１２と対象となるプログラムを特定してディアクティベーション要求を配信管理サーバ１６に送る（ステップＳ３１）。

［１．４．１０．２］ＵＩＭへのディアクティベーション要求

配信管理サーバ１６は、このディアクティベーション要求を受け取ると、データベースを参照し、ディアクティベーション要求によって特定されたＵＩＭ１２内の基本ブロックのうちディアクティベーション対象であるプログラムが格納された基本ブロックを求める。そして、そのＵＩＭ１２が装着または内蔵された移動体端末１１にディアクティベーション要求を送る（ステップＳ３２）。このディアクティベーション要求は、その対象であるプログラムが格納された基本ブロックを特定する情報を含んでいる。

ディアクティベーション要求は、移動体端末１１を介してＵＩＭ１２に送られる。ＵＩＭ１２は、ディアクティベーション要求により特定された基本ブロックに対応して用意された活性化フラグを“１”から“０”に変更する。以後、この基本ブロック内のプログラムの実行は禁止される。

［１．４．１０．３］ディアクティベーション終了応答

ＵＩＭ１２は、プログラムのディアクティベーションを終えると、その旨を示すディアクティベーション終了通知を配信管理サーバ１６に送る（ステップＳ３

３）。この通知は、ディアクティベーションが終了したプログラムを特定する情報、具体的にはそのプログラムの格納先である基本ブロックを特定する情報を含んでいる。

［１．４．１０．４］ディアクティベーション完了通知

配信管理サーバ１６は、ＵＩＭ１２からプログラムのディアクティベーション終了通知を受けると、これに基づいて、ディアクティベーションが完了したプログラムの格納先であるＵＩＭ１２の基本ブロックを求める。そして、その基本ブロックのために用意されたデータベース内の記憶領域にディアクティベーションが完了した旨の情報を登録する。

ディアクティベーション完了の登録を終えると、配信管理サーバ１６は、ディアクティベーションが完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ３４）。

［１．４．１１］削除（ユーザ希望時）

不活性化されたプログラムは、ＵＩＭ１２内のメモリ領域を無駄に使用している。このような不要なプログラムは、ユーザにとってもコンテンツプロバイダにとっても削除するのが好ましい。しかしながら、プログラムの削除をユーザに任せてしまうことはできない。ユーザが勝手にＵＩＭ１２内のプログラムを削除した場合、その事実が直ちに配信管理サーバ１６に通知されないと、プログラムが削除されているにも拘わらず、ＵＩＭの貸与料金に関する課金処理が進行してしまうからである。

そこで、本実施形態においては、ユーザがプログラムの削除を希望する場合、配信管理サーバ１６の管理下でプログラムの削除を行うようにしている。

なお、コンテンツプロバイダ側の理由による削除は、課金処理の煩雑化の関係から原則的には認めていない。

以下、ユーザの希望によりプログラムが削除される動作について図１０および図１５を参照して説明する。

［１．４．１１．１］プログラム削除要求

ユーザは、移動体端末１１の操作部２２を操作することにより、コンテンツプ

ロバイダの所定のホームページにアクセスする。そして、移動体端末１１のディスプレイ部２１の表示画面上に、図１５に示す配信メニュー画面Ｄ１１を表示させる。この配信メニュー画面Ｄ１１は、プログラムの配信を行うコンテンツプロバイダのコンテンツサーバ１９から提供されるものである。ユーザがあるプログラムの削除を意味するメニューを選択すると、移動体端末１１のディスプレイ部２１には、図１５に示すように削除の可否をユーザに問い合わせる画面Ｄ１２が表示される。

ユーザが削除を許可する操作を行うと、移動体端末１１は、プログラム（アプレット）削除要求をネットワークを介してコンテンツサーバ１９に送信する（ステップＳ４１）。この要求は、削除の対象であるプログラムを特定する情報を含んでいる。

プログラム削除要求の送信に伴い、移動体端末１１のディスプレイ部２１には、図１５に示すように削除中であることを表す画面Ｄ１３が表示される。

［１．４．１１．２］配信管理サーバへのディアクティベーション要求

コンテンツサーバ１９は、プログラム削除要求を受け取ると、配信管理サーバ１６に対してディアクティベーション要求を送る（ステップＳ４２）。このディアクティベーション要求は、プログラム削除を要求しているユーザの移動体端末１１を特定する情報と、削除対象であるプログラムを特定する情報を含んでいる。

［１．４．１１．３］ＵＩＭへのディアクティベーション要求

配信管理サーバ１６は、ディアクティベーション要求を受け取ると、データベースを参照することにより、削除対象であるプログラムが格納された基本ブロックを求める。そして、プログラム削除を要求しているユーザの移動体端末１１に対して、その基本ブロックを特定する情報を含んだディアクティベーション要求を送る（ステップＳ４３）。

このディアクティベーション要求は、移動体端末１１を介してＵＩＭ１２に送られる。ＵＩＭ１２は、ディアクティベーション要求によって特定された基本ブロックのために用意された活性化フラグを“１”から“０”に変更する。以後、当該基本ブロック内のプログラムの実行が禁止される。

［１．４．１１．４］ディアクティベーション終了応答

ＵＩＭ１２は、このようにしてプログラムのディアクティベーションを終えると、その旨を示すディアクティベーション終了通知を配信管理サーバ１６に対して送信する（ステップＳ４４）。この通知は、ディアクティベーションの行われたプログラムの格納先である基本ブロックを特定する情報を含んでいる。

［１．４．１１．５］ディアクティベーション完了通知

配信管理サーバ１６は、ＵＩＭ１２からプログラムのディアクティベーション終了通知を受けると，データベース中，ディアクティベーション終了通知によって特定されるＵＩＭ１２の基本ブロックに対応した領域に、ディアクティベーションが完了した旨の情報を登録する。

そして、配信管理サーバ１６は、プログラムのディアクティベーションが完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ４５）。

［１．４．１１．６］配信管理サーバへの削除要求

コンテンツサーバ１９は、削除対象となっているプログラムについてのディアクティベーション完了通知を配信管理サーバ１６から受け取ると、そのプログラムの削除要求を配信管理サーバ１６に送る（ステップＳ５１）。

［１．４．１１．７］ＵＩＭへの削除要求

配信管理サーバ１６は、このプログラム削除要求を受け取ると、プログラム削除の要求者であるユーザのＵＩＭ１２に対して、プログラム削除要求を送る（ステップＳ５２）。このプログラム削除要求は、削除対象であるプログラムの格納された基本ブロックを特定する情報を含んでいる。

プログラム削除要求は、移動体端末１１を介してＵＩＭ１２に送られる。ＵＩＭ１２は、プログラム削除要求によって特定された基本ブロック内のプログラムを削除する。

［１．４．１１．８］削除終了応答

ＵＩＭ１２は，プログラムの削除が終了すると、その旨を示す削除終了通知を配信管理サーバ１６に送信する（ステップＳ５３）。この削除終了通知は、プログラムの削除を行った基本ブロックおよび削除したプログラムを特定する情報を

含んでいる。これに伴い、移動体端末１１のディスプレイ部２１には、図１５に示すように削除終了であることを表す画面Ｄ１４が表示される。

［１．４．１１．９］削除完了通知

配信管理サーバ１６は、ＵＩＭ１２から削除終了通知を受けると、データベース中、削除を要求したユーザおよび削除されたプログラムの組み合わせに対応して設けられた記憶領域に、プログラムが削除された旨の情報を登録する。

そして、配信管理サーバ１６は、プログラムの削除が完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ５４）。

これに伴い、配信管理サーバは、当該削除されたプログラムについてコンテンツプロバイダに対する課金処理を行っていた場合には、以降の課金を行わないようにする。

［１．４．１２］削除（配信管理サーバ希望時）

本実施形態では、ユーザの意思によらず他の原因によりプログラムの削除が行われる場合がある。その例として、あるプログラムに使用期限が定められており、その使用期限が満了した場合がある。

以下、このような原因により、配信管理サーバの主導の下でプログラムが削除される動作について図１１を参照して説明する。

［１．４．１２．１］ＵＩＭへのディアクティベーション要求

例えば、あるプログラムの使用期限が過ぎ、プログラムを削除する必要が生じたとする。この場合、配信管理サーバ１６は、データベースを参照することにより、削除対象のプログラムが配布された全てのＵＩＭ１２と、それらにおいて削除対象のプログラムが格納されている基本ブロックを求め、各ＵＩＭ１２にディアクティベーション要求を行う（ステップＳ６１）。各ディアクティベーション要求は、削除対象プログラムが格納されている基本ブロックを特定する情報を含んでいる。

ディアクティベーション要求は、移動体端末１１を介してＵＩＭ１２に送られる。ＵＩＭ１２は、ディアクティベーション要求によって特定された基本ブロックに対応した活性化フラグを“１”から“０”に変更する。以後、当該基本ブロ

ック内のプログラムの実行を禁止させる。

［１．４．１２．２］ディアクティベーション終了応答

ＵＩＭ１２は、ディアクティベーションを終了すると、その旨を示すディアクティベーション終了通知を配信管理サーバ１６に送信する（ステップＳ６２）。

［１．４．１２．３］ディアクティベーション完了通知

配信管理サーバ１６は、削除対象であるプログラムの配布先からディアクティベーション終了通知を受け取ると、そのプログラムに対応して設けられたデータベース中の記憶領域に，ディアクティベーションが完了した旨の情報を登録する。

そして、配信管理サーバ１６は、プログラムのディアクティベーションが完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ６３）。

［１．４．１２．４］配信管理サーバへのディアクティベーション受理通知

コンテンツサーバ１９は、配信管理サーバ１６からディアクティベーション完了の通知を受け取ると、配信管理サーバ１６にディアクティベーション受理通知を送る（ステップＳ６４）。

［１．４．１２．５］ＵＩＭへの削除要求

配信管理サーバ１６は、ディアクティベーション受理通知を受け取ると、それの元となったディアクティベーション完了通知の送信元である移動体端末１１に対して、プログラムの削除要求を送る（ステップＳ７１）。この移動体端末１１に送られる削除要求は、削除対象のプログラムの格納された基本ブロックを特定する情報を含んでいる。

ＵＩＭ１２は、移動体端末１１を介して削除要求を受け取ると、これにより特定された基本ブロック内のプログラムを削除する。

［１．４．１２．６］削除終了応答

ＵＩＭ１２は、プログラムの削除を終えると、その旨を示す削除終了通知を配信管理サーバ１６に送信する（ステップＳ７２）。この通知は、プログラムの削除を行った基本ブロックを特定する情報を含んでいる。

［１．４．１２．７］削除完了通知

配信管理サーバ１６は、削除対象プログラムの全ての配布先から削除終了通知

を受け取ると、データベース中の削除対象プログラムに対応して設けられた記憶領域に、プログラムが削除された旨の情報を登録する。

そして、配信管理サーバ１６は、プログラムの削除が完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ７３）。

これに伴い、配信管理サーバは、当該削除されたプログラムについてコンテンツプロバイダに対して課金処理を行っていた場合には、以降の課金を行わないようにする。

［１．４．１２．８］配信管理サーバへの削除結果受理通知

コンテンツサーバ１９は、配信管理サーバ１６から削除完了の通知を受け取ると、配信管理サーバ１６に削除結果受理通知を送る（ステップＳ７４）。

［１．４．１３］ＵＩＭのバージョン管理に伴うプログラム配信処理

ユーザからの希望によらずコンテンツサーバ１９側が自発的にプログラムを配信する必要が生じる場合がある。例えば、配布済みのプログラムのバージョンアップが行われた場合である。

この場合において、過去にそのプログラムが配布された全てのユーザのＵＩＭ１２にバージョンアップ後のプログラムを配信すると不都合が生じる。何故ならば、移動体端末１１に様々な機種が存在するのと同様、ＵＩＭの仕様にも様々なバージョンが存在する。折角、バーションアップされたプログラムを各ＵＩＭに送ったとしても、あるバージョン以降のＵＩＭではそのプログラムを実行可能であるが、それ以前のバージョンのＵＩＭではそのプログラムを正常に実行することができないような場合が生じ得るからである。

そこで、本実施形態では、プログラムのバージョンアップが行われた場合に、ＵＩＭに対して、バージョン通知要求が送られ、これに対するＵＩＭの応答に基づいてプログラムの配信を行うか否かの判断が行われる。図１２にはこの動作が示されている。なお、ＵＩＭ１２には、バージョン通知要求に応答して当該ＵＩＭのバージョンを通知する機能をサポートしているものと、サポートしていないものとがある。図１２には、そのような機能をサポートしているＵＩＭにバージョン通知要求が送られたときの動作と、そのような機能をサポートしていないＵ

ＩＭにバージョン通知要求が送られたときの動作が示されている。

［１．４．１３．１］バージョン通知機能をサポートしているＵＩＭに関連した動作

［１．４．１３．１．１］配信管理サーバへのプログラム配信要求

コンテンツサーバ１９は、バージョンアップされたプログラムの配信を行うのに先立ち、そのプログラムを特定する情報とそのプログラムを実行可能なＵＩＭ１２のバージョンを表すバージョン情報を含んだプログラム配信要求を配信管理サーバ１６に送る（ステップＳ８１）。

［１．４．１３．１．２］ＵＩＭへのバージョン通知要求

配信管理サーバ１６は、プログラム配信要求を受け取ると、データベースを参照することにより、プログラム配信要求により特定されたプログラムが配布された全ての移動体端末１１を求め、それらの移動体端末１１にバージョン通知要求を送る（ステップＳ８２）。

［１．４．１３．１．３］バージョン通知

バージョン通知要求は移動体端末１１を介してＵＩＭ１２に送られる。ＵＩＭ１２は、バージョン通知要求を受け取ると、自己のバージョンを配信管理サーバ１６に通知する（ステップＳ８３）。

［１．４．１３．１．４］プログラム配信不可通知

配信管理サーバ１６は、各ＵＩＭ１２からバージョン通知を受け取る。そして、あるＵＩＭ１２から受け取ったバージョン通知がコンテンツサーバ１９からのバージョン情報によって示された条件を満たしていない場合には、そのＵＩＭ１２にはプログラム配信をすることが不可能である旨の通知をコンテンツサーバ１９に送る（ステップＳ８４）。

また、他のあるＵＩＭ１２から受け取ったバージョン通知がコンテンツサーバ１９からのバージョン情報によって示された条件を満たしている場合、配信管理サーバ１６は、そのＵＩＭ１２に対するプログラムの配信を行う。この場合の動作は、既に図６および図８を参照して説明した通りである。

［１．４．１３．２］バージョン通知機能をサポートしていないＵＩＭに関連し

た動作

［１．４．１３．２．１］配信管理サーバへのプログラム配信要求

コンテンツサーバ１９は、上述と同様、配信管理サーバ１６にプログラムの配信要求を送る（ステップＳ９１）。

［１．４．１３．２．２］ＵＩＭへのバージョン通知要求

配信管理サーバ１６は、移動体端末１１のＵＩＭ１２に対して、バージョン通知要求を送る（ステップＳ９２）。

［１．４．１３．２．３］タイマカウント

この場合において、ＵＩＭ１２は、バージョン通知通信機能をサポートしていないので、応答することはない。

従って、配信管理サーバ１６は、タイマを監視し、所定のタイムアウト時間が満了した場合には（ステップＳ９３）、再度移動体端末１１のＵＩＭ１２に対して、バージョン通知要求を行う（ステップＳ９４）。そしてリトライカウンタの値を１だけ増加させる。

同様に配信管理サーバ１６は、タイマを監視し、所定のタイムアウト時間が満了した場合には（ステップＳ９５）、再度移動体端末１１のＵＩＭ１２に対して、バージョン通知要求を行う（ステップＳ９６）。そしてリトライカウンタの値を１だけ増加させる。

［１．４．１３．２．４］プログラム配信不可通知

再び、同様に配信管理サーバ１６は、タイマを監視し、所定のタイムアウト時間が満了した場合には（ステップＳ９７）、再度移動体端末１１のＵＩＭ１２に対して、バージョン通知要求を行う（ステップＳ９８）。そしてリトライカウンタの値を１だけ増加させる。

そして、リトライカウンタの値が所定の値（この例の場合は３）となったとき、配信管理サーバ１６は、ＵＩＭ１２のバージョンがコンテンツサーバ１９から通知されたバージョンの条件を満たしていないと見なしてコンテンツサーバ１９に対してプログラム配信不可通知を行う（ステップＳ８４）。

これによりコンテンツサーバ１９は、配信を希望したプログラムが配信できな

いことを把握することとなる。

［１．４．１４］ＵＩＭのメモリ容量制限に伴うプログラム配信処理

ＵＩＭ１２のメモリ容量には限界があるため、コンテンツサーバ１９側でプログラムの配信を希望したとしても配信ができない場合が起こりうる。図１３はそのような場合の動作例を示している。以下、この動作例について説明する。

［１．４．１４．１］配信管理サーバにおけるリジェクト

コンテンツサーバ１９は、配信するプログラムを添付して、ＵＩＭ１２へのプログラム配信要求を配信管理サーバ１６に送る（ステップＳ１０１）。

配信管理サーバ１６のデータベースには、ＵＩＭ１２毎にそのメモリの状況を示す情報が登録されている。配信管理サーバ１６は、あるＵＩＭ１２へのプログラム配信要求を受け取ると、データベースを参照し、そのＵＩＭ１２の基本ブロックに空きがない、あるいは、空いている基本ブロックはあるがプログラムを記憶するには容量が小さい（ＵＩＭのバージョンによって異なる場合が想定されるため）など、プログラムの配信を阻害する理由があるか否かを判別する。

そして、配信管理サーバ１６は、プログラムの配信ができない場合には、メモリ容量不足によるプログラム配信不可通知をコンテンツサーバ１９に送る（ステップＳ１０２）。

これによりコンテンツサーバ１９は、配信を希望したプログラムが配信できないことを把握する。

［１．４．１４．２］ＵＩＭにおけるリジェクト

配信管理サーバ１６のデータベースには、ＵＩＭ１２毎にそのメモリの容量と利用状態が登録されている。しかしながら、何らかの理由により実際のＵＩＭにおけるメモリの利用状態と、配信管理サーバ１６のデータベースに登録されたメモリの利用状態とが異なる場合がある。このような場合に行われる動作について説明する。

まず、コンテンツサーバ１９は、プログラムを添付したプログラム配信要求を配信管理サーバ１６に送る（ステップＳ１１１）。

配信管理サーバ１６は、データベースを参照し、配信先のＵＩＭ１２の基本ブ

ロックに空きがあり、かつ、基本ブロックの容量が十分であるか否かを判断する。

この判断結果が「ＹＥＳ」である場合、配信管理サーバ１６は、プログラムを添付した書込要求をＵＩＭ１２に送る（ステップＳ１１２）。

書込要求を受け取ったＵＩＭ１２は、書込要求に添付されたプログラムをいずれかの基本ブロックに格納可能であるか否かを判断する。そして、この判断結果が「ＮＯ」である場合、ＵＩＭ１２は、配信管理サーバ１６に対してメモリ容量不足によるプログラム配信不可通知を送る（ステップＳ１１３）。

配信管理サーバ１６は、プログラム配信不可通知を受け取ると、メモリ容量不足によるプログラム配信不可通知をコンテンツサーバ１９に送る（ステップＳ１１４）。

コンテンツサーバ１９は、この通知により、配信希望先であるＵＩＭにプログラムを配信できないことを把握することができる。

ＵＩＭ１２のメモリの書込エラーやメモリデバイスそのものの故障により、基本ブロックへのプログラムの格納を行うことができない場合もある。この場合、以上説明したものと全く同じ動作が行われる。図１４はその動作を示している。図１４におけるステップＳ１２１～Ｓ１２４は、図１３のステップＳ１１１～Ｓ１１４に対応しており、その動作内容は全く同じである。

［１．４．１５］具体的動作例

以下、本実施形態の具体的動作例について説明する。

［１．４．１５．１］ＵＩＭに格納されたプログラムの実行

この動作例では、ＵＩＭ１２の基本ブロック４０－１に“○○鉄道”プログラムが格納されているものとする。

ユーザは、移動体端末１１の操作部２２を操作することにより、“○○鉄道”プログラムを配信したコンテンツプロバイダのホームページにアクセスし、ディスプレイ部２１の表示画面に図１６に示すような配信メニュー画面Ｄ２１を表示させる。この配信メニュー画面Ｄ２１は、コンテンツプロバイダのコンテンツサーバ１９から提供されるものである。ユーザは、この配信メニュー画面Ｄ２１の表示メニューの中から定期券の購入に関するものを選択する操作を行うと、定期

券の購入要求が移動体端末１１からネットワークを介してコンテンツサーバ１９に送信される。

この結果、ダウンロード画面Ｄ２２がコンテンツサーバ１９から移動体端末１１に送られ、ディスプレイ部２１に表示される。このダウンロード画面Ｄ２２は、定期券と同一の金銭的価値を有する幾つかのバリューデータのメニューを含んでいる。

ユーザがそれらの中から所望のバリューデータを選択すると、この選択されたバリューデータを要求する情報が移動体端末１１からコンテンツサーバ１９に送られる。

その後、コンテンツサーバ１９は、決済方法を選択させるための画面のデータを移動体端末１１に送る。この結果、画面Ｄ２３が移動体端末１１によって表示される。ユーザは、画面Ｄ２３内のメニューの中から“ＵＩＭメニューから選択”を選択することにより、ＵＩＭ１２内のプログラムを利用して決済を行うことができる。すなわち、この選択を行うと、その旨の通知がＵＩＭ１２に送られる。この通知を受けたＵＩＭ１２の制御部は、基本ブロック４０－１～４０－６に格納されているプログラムのリストを移動体端末１１に送り返す。そして、このリストを含む画面Ｄ２４が移動体端末１１のディスプレイ部２１に表示される。ユーザがこのリストに掲げられたプログラムの中から決済に関するものを選択すると、ＵＩＭ１２によってそのプログラムが実行され、決済処理が行われる。

この決済処理が例えば基本ブロック４０－２のプログラム領域４１内のプログラムの実行により行われるととすると、同決済処理では、同一基本ブロック４０－２のデータ領域４２が用いられる。

コンテンツサーバ１９は、この決済処理が終わったことを検知すると、上述した定期券購入要求によって要求された定期券のバリューデータを移動体端末１１に送る。このバリューデータは、乗車区間、有効期限、ユーザ氏名、ユーザの年齢等の情報を含んでおり、移動体端末１１からＵＩＭ１２に送られる。ＵＩＭ１２では、このバリューデータが“○○鉄道”プログラムによって使用されるべきものであることから、同プログラムに対応した基本ブロック４０－１のデータ領

域４２にバリューデータを格納する。

［１．４．１５．２］ネットワークを利用した通信販売

この動作例においては、通信販売のためのプログラムがＵＩＭ１２の基本ブロック４０－２に格納されているものとする。

ユーザは、移動体端末１１の操作部２２を操作することにより、コンテンツプロバイダのホームページにアクセスし、移動体端末１１のディスプレイ部２１に図１７に示す配信メニュー画面Ｄ３１を表示させる。この配信メニュー画面Ｄ３１は、ネットワークを利用した通信販売（いわゆる、ｅ－コマース）のサービスを提供するコンテンツプロバイダのコンテンツサーバ１９から提供されるものである。ユーザが配信メニュー画面Ｄ３１に挙げられた商品の中から所望の商品（図１７では、すき焼き用松阪牛１キログラム５，０００円）を選択すると、購入要求が移動体端末１１からネットワークを介してコンテンツサーバ１９に送信される。

購入要求を受け取ったコンテンツサーバ１９は、決済方法の選択画面Ｄ３２を移動体端末１１に送り返す。この結果、選択画面Ｄ３２がディスプレイ部２１に表示させる。

この選択画面Ｄ３２に挙げられた決済方法の中から例えば、「ＸＸ銀行」が選択されると、ＵＩＭ１２の基本ブロック４０－３に格納されているＸＸ銀行の決済プログラムがＵＩＭ１２内の制御部３０によって起動され、決済画面Ｄ３４が表示される。

そこで、ユーザが決済情報をとして、暗証番号を入力すると、移動体端末１１は、通信部３４およびネットワークを介してＸＸ銀行の決済サーバに接続を試み、アクセス中画面Ｄ３５が表示される。

そして、認証が完了すると、引き落とし額確認画面Ｄ３６が表示される。

ユーザがこれを確認し、その旨の入力を行うと、再び、移動体端末１１は、通信販売を行っているコンテンツプロバイダの入金確認画面Ｄ３７を表示し、商品の届け日などを表示する。

［１．４．１５．３］定期券使用（改札通過：マニュアル起動時）

本実施形態においては、ＵＩＭ１２に適切なプログラムを格納しておくことにより移動体端末１１を定期券代わりに使用することができる。以下、その動作例を説明する。

まず、ユーザがＵボタン２３を押し下げると、図１８に示すＵＩＭメニュー画面Ｄ４１がディスプレイ部２１に表示される。次にユーザは、定期券を利用する「○○鉄道」を選択する。これにより、ＵＩＭ１２の制御部３０は、基本ブロック４０－１内の○○鉄道のプログラムを実行し、ディスプレイ部２１にメニュー画面Ｄ４２を表示させる。

画面Ｄ４２が表示されたとき、ユーザが「４．アプリケーション自動起動設定」を選択すると、自動起動設定確認画面Ｄ４３が表示され、ユーザに選択を促す。

ここで、ユーザが「はい」を選択すると、自動起動が設定される。一方、「いいえ」を選択すると、自動起動は設定されない。

鉄道会社の改札口には、改札用リーダ／ライタ装置が配置されている。ユーザは、改札口を通過するとき、事前に次のような操作をする。

まず、ユーザはＵボタン２３を押し下げ、図１９に示すＵＩＭメニュー画面Ｄ４１をディスプレイ部２１に表示させる。次にユーザは、定期券を利用する「○○鉄道」を選択する。これにより、ＵＩＭ１２の制御部３０は、基本ブロック４０－１内の○○鉄道のプログラムを実行し、ディスプレイ部２１にメニュー画面Ｄ４２を表示させる。そして、ユーザは、「１．定期券」を選択すると、○○鉄道プログラムの一部である定期券プログラムが制御部３０によって起動される。そして、制御部３０は、この定期券プログラムに従い、改札処理のための通信を改札用リーダ／ライタ装置と行う。この通信が例えば共通鍵暗号方式により行われるとした場合、改札処理は次の手順により行われる。

（１）お互いに通信相手を確認する。

（２）改札用リーダ／ライタが移動体端末１１に定期券に関する情報の送信を要求する。

（３）移動体端末１１が定期券に関する情報を共通鍵で暗号化して改札用リーダ／ライタに送信する。このとき移動体端末１１のディスプレイ部に定期券情報の

表示画面Ｄ５３を表示させる。

（４）改札用リーダ／ライタは、受信した定期券に関する情報を復号化し、正規ユーザである場合には、通過を許可すべ、改札口ゲートを開く。

これに伴い、ユーザに対するお礼のメッセージ画面Ｄ５４などがディスプレイ部２１に表示される。

以上の説明は、定期券の場合であったが、移動体端末１１をプリペイドカードとして機能ささえる場合には、上記（４）の処理において、使用金額差し引き後の金額に相当するバリューデータとしてデータ領域４２を更新すればよい。

［１．４．１５．４］定期券使用（改札通過：自動起動時）

図１８に示す画面Ｄ４３が表示されたときにユーザが「はい」を選択し、自動起動が設定されたとする。この場合の動作は次のようになる。すなわち、自動起動の設定が行われた移動体端末１１が駅の改札口に接近すると、改札用リーダ／ライタ装置から送信されるポーリング信号が移動体端末１１によって受信される。この結果、ＵＩＭ１２では、○○鉄道プログラムの一部である定期券プログラムが制御部３０によって自動起動され、上記マニュアル起動の場合と同様な改札処理が行われる。

［１．５］第１実施形態の効果

以上説明したように、本実施形態によれば、記憶モジュールの記憶領域を分割して各プログラムを格納して使用する場合にも、移動体端末側は、通信機能をＵＩＭに提供するだけであり、移動体端末側に余計な負担をかけることがないので、移動体端末の本来の機能を損ねることがない。

また、プログラムの格納、アクティベーション、ディアクティベーション、削除などは、移動体端末には行わせることなく、配信管理サーバの制御下で行われるため、移動体端末側で処理を行うことはできず、セキュリティを確保しつつ、ユーザの使い勝手を向上することができる。

［２］第２実施形態

上記第１実施形態においては、ＵＩＭ１２によって実行されるプログラムは、

同ＵＩＭ内の基本ブロック４０－１～４０－６に格納された。本実施形態において、ＵＩＭ１２は、実行するプログラムのすべてを必ずしも基本ブロックに格納する必要はない。

［２．１］第２実施形態の構成

図２１はこの発明の第２実施形態であるプログラム配信システムの構成を示すブロック図である。

図２１には、ＵＩＭ１２と、コンテンツサーバ１９－１～１９－６および１９Ｘと、配信管理サーバ１６Ａが示されている。配信管理サーバ１６Ａは、上記第１実施形態における配信管理サーバ１６に対し、本実施形態特有の機能が追加されている。コンテンツサーバ１９－１～１９－６および１９Ｘは、上記第１実施形態におけるコンテンツサーバ１９と同様な役割を果たす。本実施形態に係るシステムは、上記第１実施形態における認証サーバ等も有しているが、図２１では省略されている。

本実施形態におけるＵＩＭ１２は、第１実施形態におけるアプリケーション領域１２Ｂに代えて、図２２に示すアプリケーション領域１２Ｃを備えている。このプログラム記憶領域１２Ｃは、７個の基本ブロック４０－１～４０－７および１個のフリー基本ブロック４０－Ｆ１に分けられている。

各基本ブロック４０－１～４０－７およびフリー基本ブロック４０－Ｆ１は、それぞれプログラム領域４１およびデータ領域４２を備えている。

プログラム領域４１は、プログラム（アプリケーションあるいはアプレット）を格納する。データ領域４２は、同一の基本ブロックあるいはフリー基本ブロックにおけるプログラム領域４１に格納されたプログラムが使用するデータを格納する。

この場合において、基本ブロック４０－１～４０－７およびフリー基本ブロック４０－Ｆ１は、互いに独立しており、原則的には、あるブロックのプログラム領域４１に格納されたプログラムが他のブロックのデータ領域４２にアクセスすることはできない。この点は上記第１実施形態と同様である。また、プログラム領域４１に格納されたプログラムについては、配信管理サーバ１６Ａを経由しな

いかぎり配信、削除などを行うことはできないが、データ領域４２については、ＡＴＭから電子マネーをダウンする場合のように、配信管理サーバ１６Ａ経由あるいはローカルな端末を介して直接操作することが可能となっている。この点も上記第１実施形態と同様である。

本実施形態において、基本ブロック４０－１～４０－７に格納されるプログラムについては、配信管理サーバ１６Ａによって配信状態が管理される。しかし、フリー基本ブロック４０－Ｆ１については、配信管理サーバ１６Ａではなく、ユーザの責任において管理される。

上記第１実施形態において配信管理サーバ１６は、移動体端末１１からの配信要求に応じてコンテンツサーバ１９から送信されたプログラムをＵＩＭ１２に送った。本実施形態における配信管理サーバ１６Ａは、移動体端末１１からプログラムの配信要求を受け付け、必要に応じてコンテンツサーバにアクセスしてそのプログラムを取得し、移動体端末１１のＵＩＭ１２に配信する。本実施形態における配信管理サーバ１６Ａは、コンテンツサーバからＵＩＭ１２へのプログラム配信の中継およびその管理を行うという点において上記第１実施形態の配信管理サーバ１６と共通している。しかし、本実施形態における配信管理サーバ１６Ａは、このような中継および管理をするだけに止まらない。すなわち、配信管理サーバ１６Ａは、ＵＩＭ１２のユーザのためにプログラムまたはその所在を示す情報を格納する手段を有しており、この手段によって格納されている範囲内のプログラムについては、ユーザは配信管理サーバ１６Ａを通じてそのプログラムを取得することができる。この意味で配信管理サーバ１６Ａは、ＵＩＭ１２のためのいわばキャッシュメモリとしての役割を果たすものである。

配信管理サーバ１６Ａは、ＵＩＭ１２に対するプログラムの配信の管理とこのようなキャッシュメモリ的な機能を果たすために、配信状態管理部５０を備えている。この配信状態管理部５０は、ユーザ情報格納部５１と、プログラム情報格納部５２とを備えている。

プログラム情報格納部５２は、ＵＩＭ１２に配信可能なプログラム本体またはプログラムに対応したＵＲＬを格納している。ここで、ＵＲＬは、そのプログラ

ムがコンテンツサーバ１９－１～１９－６のうちどのコンテンツサーバのどのアドレスにあるかを表す情報である。あるプログラムについて、ＵＲＬ情報あるいはプログラム本体のいずれをプログラム情報格納部５２に格納するかは、プログラム情報格納部５２の記憶容量に基づいて定めるか、あるいは記憶容量が十分である場合には、配信サーバを運営するコンテンツプロバイダの希望により選択させるように構成することが可能である。

プログラム情報格納部５２に新規なプログラムまたはそのＵＲＬが格納される機会として、例えば、あるユーザの移動体端末１１からプログラムの配信要求が送られ、この配信要求に応えるようなプログラムまたはそのＵＲＬがプログラム情報格納部５２に格納されていない場合が挙げられる。かかる場合、プログラム情報格納部５２は、移動体端末１１からの要求に従い、コンテンツサーバにアクセスし、ユーザが望むプログラムを取得して格納する。

ユーザ情報格納部５１は、本システムが適用されるｎ人（ｎは複数）のユーザに対応付けられたｎ個のユーザ個別情報格納部５３－１～５３－ｎを備えており、各ユーザ個別情報格納部５３－ｋは、実配信情報格納部５４と、仮想配信情報格納部５５とを備えている。

ユーザ個別情報格納部５３－ｋにおける実配信情報格納部５４は、ユーザｋのＵＩＭ１２に実際に配信されたプログラムに対応したポインタデータを格納する。このポインタデータは、そのプログラムそのものまたはそのプログラムのＵＲＬが格納されているプログラム情報格納部５２内のエリアを示すポインタである。この実配信情報格納部５４を有しているため、配信管理サーバ１６Ａは、ＵＩＭ１２の基本ブロック４０－１～４０－７にあるプログラムが万が一消去された場合でも、直ちに再配信を行うことができる。

また、ユーザ個別情報格納部５３－ｋにおける仮想配信情報格納部５５は、ユーザｋのＵＩＭ１２に実際に配信されてはいないが、ユーザｋが希望する場合にＵＩＭ１２に直ちに提供可能なプログラムに対応したポインタデータを格納する。ＵＩＭ１２のユーザは、仮想配信情報配格納部５５を利用した次のようなサービスを受けることができる。

ａ．ＵＩＭ１２への配信を希望するプログラムのポイントデータを取り敢えず仮想配信情報格納部５５に格納してもらう。ユーザは、仮想配信情報格納部５５にポインタデータが格納されたプログラムの配信が必要になったときに、移動体端末１１を用いて配信管理サーバ１６Ａにその旨の要求を送る。配信管理サーバ１６Ａは、要求されたプログラムのポインタデータを仮想配信情報格納部５５から読み出し、そのポインタデータによって特定されたプログラムを取得してＵＩＭ１２に配信する。この場合、ＵＩＭ１２に配信されたプログラムのポインタデータは、仮想配信情報記憶部５５から実配信情報格納部５４に移動される。

ｂ．ＵＩＭ１２内の基本ブロックは数に限りがある。従って、基本ブロックが全てふさがっており、配信対象であるプログラムを格納可能な空き状態の基本ブロックがないという事態が起こりうる。そのような場合、配信管理サーバ１６Ａは、実配信情報格納部５４内の記憶領域のうちＵＩＭ１２内のある基本ブロック４０－Ｘに対応した記憶領域からポインタデータを読み出し、これを仮想配信情報格納部５５に移す。そして、配信対象であるプログラムをＵＩＭ１２に送って、基本ブロック４０－Ｘに書き込ませ、そのプログラムのポインタデータを実配信情報格納部５４内の基本ブロック４０－Ｘに対応した記憶領域に書き込む。このような処理により、ユーザは、基本ブロックが満杯状態であるときにも、配信要求をしてプログラムを取得し、基本ブロックに格納することができる。その際に基本ブロックから追い出されたプログラムについては、必要があれば、再度、配信管理サーバ１６Ａに要求し、上記ａの処理を行ってもらえばよい。

次に、フリー基本ブロック４０－Ｆ１に対応した配信管理サーバ１６Ａの機能について説明する。既に述べたように、フリー基本ブロック４０－Ｆ１に関しては、配信管理サーバ１６は、プログラムの配信の管理をしない。ユーザは、移動体端末１１を操作することにより、自由にフリー基本ブロック４０－Ｆ１へのプログラムの登録、プログラムの削除を行うことができる。

ユーザ個別情報格納部５３の実配信情報格納部５４には、ＵＩＭ１２内の基本ブロック４０－Ｆ１に対応した記憶領域が設けられている。しかし、この領域には、何らかのプログラムのポインタデータが記憶されることはなく、基本ブロッ

ク４０－Ｆ１に対するプログラムの登録あるいは削除の回数などのデータ若しくはそのプログラムのＵＲＬ情報等が格納される。なお、フリー基本ブロック４０－Ｆ１に何も格納されていない場合には、その旨を表すデータ（Ｎｕｌｌデータ等）をこの領域に格納するように構成してもよい。

ＵＩＭ１２のフリー基本ブロック４０－Ｆ１にあるプログラムは、それが万が一消去された場合、上記基本ブロック４０－１～４０－７に格納されているプログラムとは異なり、ユーザ自身が再登録を行わない限り、そのままの状態となる。

一方、フリー基本ブロック４０－Ｆ１にあるプログラムを一時的にユーザが他のプログラムに変更したい場合には、ユーザ自身が書き換えることによりいつでも変更が可能となっている。

この場合において、配信管理サーバ１６Ａは、フリー基本ブロック４０－Ｆ１にプログラムが格納されたとしても、課金処理を行うことはない。

フリー基本ブロック４０－Ｆ１は、ユーザの希望に応じて基本ブロック４０－１～４０－７と同一に取り扱うように変更することが可能である。すなわち、変更前は、７個の基本ブロック４０－１～４０－７および１個のフリー基本ブロック４０－Ｆ１を８個の基本ブロック４０－１～４０－８として利用させることが可能である。

この場合には、配信管理サーバ１６Ａは、ＵＩＭ１２のシステム領域１２Ａ（図４参照）にフリー基本ブロック４０－Ｆ１を基本ブロック４０－８に変更した旨の情報を書き込む。また、配信管理サーバ１６Ａは、それまでフリー基本ブロック４０－Ｆ１に対応したものとして扱っていた実配信情報格納部５４内の領域を、以後は、基本ブロック４０－８に対応した領域として扱い、この領域を用いて、基本ブロック４０－１～４０－７について行われているものと同じ管理を開始する。

なお、このようにユーザが一旦基本ブロック４０－８に変更した基本ブロックを再びフリー基本ブロック４０－Ｆ１に戻すことも可能である。基本ブロック４０－１～４０－７については、フリー基本ブロックに変更することはできない。

［２．２］配信管理サーバの構成

図２３に配信管理サーバ１６Ａの構成を示す。

配信管理サーバ１６Ａは、大別すると、伝送制御部６１と、上述したユーザ情報格納部５１と、上述したプログラム情報格納部５２と、セキュア通信制御部６２と、を備えている。

伝送制御部６１は、外部のコンテンツサーバ１９－１～１９－６あるいは移動体端末１１との間（コンテンツサーバ１９－１～１９－６－移動体端末１１相互間も含む。）の伝送制御を行う。また、伝送制御部６１は、ユーザ情報格納部５１、プログラム情報格納部５２およびセキュア通信制御部６３相互間の伝送制御を行う。さらに伝送制御部６１は、配信状態管理部５０、ユーザ情報格納部５１、プログラム情報格納部５２およびセキュア通信制御部６３の制御並びに配信状態管理部５０、ユーザ情報格納部５１、プログラム情報格納部５２およびセキュア通信制御部６３における各種処理の実行要求などを行う。

プログラム情報格納部５２は、ＵＩＭ１２の基本ブロック４０－１～４０－７に配信を許可しているプログラムに対するポータルサイト（Portal site）として実質的に機能している。

セキュア通信制御部６３は、コンテンツサーバ１９－１～１９－６から送付された情報（暗号化されたプログラムなど）の認証、各ＵＩＭが保持している秘密鍵の鍵対となる公開鍵の保持あるいはコンテンツサーバ１９－１～１９－６に対する公開鍵の発行管理などを行う。

［２．３］第２実施形態の動作

［２．３．１］ユーザ情報格納部への登録

図２１に示す例において、コンテンツサーバ１９－１～１９－６は、配信管理サーバ１６Ａの管理下にある。ユーザは、これらのコンテンツサーバに格納されたプログラム（アプレット）を利用したい場合、そのプログラムを配信管理サーバ１６Ａのユーザ情報格納部５１に登録する必要がある。以下、図２４を参照し、この登録処理について説明する。

まず、ユーザは、登録可能なプログラムのメニューリストの要求を移動体端末１１から配信管理サーバ１６Ａに送る。この要求は、配信管理サーバ１６Ａの伝

送制御部６１を介してプログラム情報格納部５２に送られる（ステップＳ１３１）。

この要求を受けたプログラム情報格納部５２は、登録可能なプログラム、具体的にはプログラム情報格納部５２にプログラム本体またはＵＲＬが格納されている全プログラムのメニューリストを作成し、伝送制御部６１を介して移動体端末１１に送信する（ステップＳ１３２）。

このメニューリストは、移動体端末１１によって受信され、ディスプレイ部２１に表示される。この状態において、ユーザは、操作部２２を操作し、配信管理サーバ１６Ａから所望のプログラムについてのコメントを取得してディスプレイ部２１に表示させることができる。

ユーザが操作部２２を操作することにより、配信を要求するプログラムが確定すると、移動体端末１１は、そのプログラムを特定する情報を含んだ登録要求を配信管理サーバ１６Ａのプログラム情報格納部５２に送信する（ステップＳ１３３）。

プログラム情報格納部５２は、このプログラム登録要求に基づき、ユーザが要求しているプログラムのユーザ情報格納部５１への登録を行う（ステップＳ１３４）。

このステップＳ１３４の動作を詳しく述べると次の通りである。まず、上記登録要求が、例えば、あるユーザｋのＵＩＭ１２が内蔵または装着された移動体端末１１からの登録要求であったとする。この場合、プログラム情報格納部５２は、登録要求に基づき、ユーザが要求しているプログラムを判別し、プログラム情報格納部５２内の各領域のうちそのプログラムの所在を表すＵＲＬ情報あるいはそのプログラム本体を格納している領域を特定するポインタデータを求める。このようにしてユーザが要求しているプログラムのポインタデータが得られると、プログラム情報格納部５２は、ユーザｋに対応したユーザ個別情報格納部５３－ｋの実配信情報格納部５４の各領域の記憶内容を参照することにより、ユーザｋのＵＩＭ１２の各基本ブロックのうち空き状態である基本ブロック４０－Ｘ（１≦Ｘ≦７）を求める。そして、実配信情報格納部５４の各領域のうちこの基本ブロ

ック４０－Ｘに対応する領域に、ユーザが要求しているプログラムのポインタデータを登録する（ステップＳ１３４）。ここで、ユーザｋのＵＩＭ１２に空いている基本ブロック４０－Ｘ（１≦Ｘ≦７）が存在しない場合もあり得る。かかる場合、プログラム情報格納部５２は、ユーザが指定したあるいは自動的に設定した仮想配信情報格納部５５にポインタデータを登録する。

ところで、ステップＳ１４１において、メニューリストの中に所望のプログラムがない場合がある。かかる場合、ユーザは、移動体端末１１を操作してプログラム情報格納部５４に所望のコンテンツサーバへのアクセスを要求することができる。この場合、プログラム情報格納部５４は、ユーザからの要求に従い、ユーザが望むコンテンツサーバからプログラムまたはそのＵＲＬを取得し、プログラム情報格納部５４内の空いているエリアに保持する。この場合、取得したプログラムまたはＵＲＬの所在を示すポインタデータの実配信情報格納部５４への登録は、上述と同様の手順で行われる。

このようにして、ユーザが要求しているプログラムの登録が終了すると、配信管理サーバ１６Ａは、当該ユーザあるいは当該プログラムの配信元のコンテンツプロバイダなどを対象とした課金処理を開始する。

続いて、ユーザ情報格納部５１は、伝送制御部６１を介して、移動体端末１１に登録通知を送る（ステップＳ１３５）。

移動体端末１１は、この登録通知を受け取ると、登録応答を配信管理サーバ１６Ａに送る（ステップＳ１３６）。

ユーザ情報格納部５１は、ユーザｋのＵＩＭ１２が内蔵または接続された移動体端末１１からの登録応答を伝送制御部６１を介して受け取ると、そのユーザｋのためにポインタデータの登録を行ったプログラムを格納しているコンテンツプロバイダ１９を求め、そのコンテンツサーバ１９にアクティベーション許可要求を送る（ステップＳ１３７）。

このアクティベーション許可要求を受け取ったコンテンツサーバ１９は、プログラムの利用契約を承認すべく、アクティベーション許可をユーザ情報格納部５１に送る（ステップＳ１３８）。これによりユーザ情報格納部５１は、ユーザｋ

に対応したユーザ個別情報格納部５３－ｋの実配信情報格納部５４の各領域のうち基本ブロック４０－Ｘに対応した領域に記憶されたポインタデータの使用が許可されたものとして取り扱う。

そして、ユーザ情報格納部５１は、移動体端末１１に対し登録が完了した旨の登録完了通知を送る（ステップＳ１３９）。この登録完了通知は、ユーザ情報格納部５１へのポインタデータの登録が行われているプログラムの一覧である登録リストを含んでいる。

ユーザは、移動体端末１１のディスプレイ部２１によりこの登録リストを確認することができる。

［２．３．１．１］ＵＩＭの基本ブロックへの登録（コンテンツサーバがプログラムを保持している場合）

登録リストを受け取ったユーザｋは、自らが登録を要求したプログラムの配信およびＵＩＭ１２内への書込を要求することができる。図２５を参照し、この場合の動作について説明する。

ユーザｋは、登録リストの中から配信を望むプログラムを選択する操作を行うと、そのプログラムが登録リスト中の何番目に位置するかを示す登録リスト内ポインタを含んだ配信要求が移動体端末１１から配信管理サーバ１６Ａのユーザ情報格納部５１に送られる（ステップＳ１４１）。

ユーザ情報格納部５１は、ユーザｋの移動体端末１１から配信要求を受け取ると、ユーザ個別情報格納部５３－ｋの実配信情報格納部５４の各領域のうち配信要求に含まれる登録リスト内ポインタに対応した領域から、配信要求の対象であるプログラムのＵＲＬまたはプログラム本体の格納先を特定するポインタデータを読み出す。そして、このポインタデータを含む配信要求をプログラム情報格納部５２に送る（ステップＳ１４２）。

プログラム情報格納部５２は、この配信要求中のポインタデータによって特定された領域を参照する。そして、当該領域にプログラムのＵＲＬが格納されている場合には、そのＵＲＬを用いて、コンテンツサーバ１９にプログラムの配信を要求する（ステップＳ１４３）。

コンテンツサーバ１９は、この配信要求を受け取ると、認証サーバ１８に対して、配信管理サーバ公開鍵を要求する（ステップＳ１４４）。

認証サーバ１８は、コンテンツサーバ１９がＵＩＭ１２への書き込みが許可された者である場合には、配信管理サーバ公開鍵をコンテンツサーバ１９に発行する（ステップＳ１４５）。

コンテンツサーバ１９は、この配信管理サーバ公開鍵を用いた暗号化をプログラムに施し、証明書付きプログラムとして配信管理サーバ１６Ａのセキュア通信制御部６２に配信する（ステップＳ１４６）。

セキュア通信制御部６２は、配信管理サーバ公開鍵と対をなす配信管理サーバ秘密鍵を記憶しており、この鍵を用いて、証明書付きプログラムの復号化を行う。この復号化が成功すると、平文のプログラムが得られる。

セキュア通信制御部６２は、配信先であるＵＩＭ１２に対応したＵＩＭ公開鍵を認証サーバ（第１実施形態参照）から取得し、このＵＩＭ公開鍵によりプログラムを暗号化してＵＩＭ１２に送る。ＵＩＭ１２では、ＵＩＭ公開鍵と対をなすＵＩＭ秘密鍵を用いてプログラムの復号化が行われ、この復号化が成功すると、平文によるプログラムが得られる。ＵＩＭ１２は、このプログラムを基本ブロック４０－Ｘに書き込む（ステップＳ１４７）。なお、ＵＩＭ１２は、配信管理サーバ１６Ａ内のプログラム情報格納部５２が用いているのと同じアルゴリズムにより基本ブロック４０－Ｘを求める。従って、このステップＳ１４７では、図２４のステップＳ１３４において求められたものと同じ基本ブロック４０－Ｘが求められる。なお、図２４のステップＳ１３９において配信管理サーバ１６Ａから送信される登録完了通知に、ステップＳ１３４において求められた空き状態の基本ブロック４０－Ｘを特定する情報を含め、図２５のステップＳ１４７では、この情報により特定された基本ブロック４０－Ｘにプログラムを格納するようにしてもよい。

ＵＩＭ１２は、プログラムの書き込みが終了すると、その旨を示す書込終了通知を配信管理サーバ１６のセキュア通信制御部６２に送信する（ステップＳ１４８）。この書込終了通知は、プログラムの書込が行われた基本ブロック４０－Ｘ

を特定する情報を含んでいる。

配信管理サーバ１６のセキュア通信制御部６２がこの書込終了通知を受けると、ユーザ情報格納部５１は、ＵＩＭ１２に書き込んだプログラムの実行の許可を要求すべく、アクティベーション要求をコンテンツサーバ１９に送る（ステップＳ１４９）。

このアクティベーション要求を受け取ったコンテンツサーバ１９は、アクティベーション許可をユーザ情報格納部５１に送る（ステップＳ１５０）。

このアクティベーション許可を受け取ったユーザ情報格納部５１は、ＵＩＭ１２にアクティベーション指示を送る（ステップＳ１５１）。

ＵＩＭ１２では、このアクティベーション指示が受信されると、プログラムを書き込んだ基本ブロック４０－Ｘに対応した活性化フラグが“０”から“１”に切り換えられ、以後、当該基本ブロック内のプログラムの実行が可能となる。

ＵＩＭ１２は、プログラムのアクティベーションが終了すると、その旨を示すアクティベーション応答通知をプログラムを特定する情報（例えば、基本ブロック４０－Ｘを特定する情報）とともに配信管理サーバ１６Ａのユーザ情報格納部５１に送信する（ステップＳ１５２）。

ユーザ情報格納部５１は、ユーザｋのＵＩＭ１２からアクティベーション応答通知を受けると、ユーザ個別情報格納部５３－ｋの実配信情報格納部５４の各領域のうち基本ブロック４０－Ｘに対応した領域を求める。この領域には、ユーザｋのＵＩＭ１２に基本ブロック４０－Ｘに書き込まれたプログラムに対応したポインタデータが既に書き込まれている。そして、この領域に、既にあるポインタデータと同居するような形でアクティベーションが完了した旨の情報が書き込まれる。このような動作が行われるため、配信管理サーバ１６Ａは、ユーザ情報格納部５１の各エリアを参照することにより全てのＵＩＭ１２の基本ブロック４０－１～４０－７について、活性化が行われているかどうかを把握することができる。

ユーザ情報格納部５１は、アクティベーションが完了した旨の情報の書込を終えると、移動体端末１１に登録完了の旨をプログラムリストとして通知し、ユー

ザに以後、プログラムの実行が可能である旨を通知するとともに、処理を終了する（ステップＳ１５３）。

配信管理サーバ１６Ａは、プログラムのアクティベーションが完了した旨の通知をコンテンツサーバ１９に送る（ステップＳ１５４）。

［２．３．１．２］ＵＩＭの基本ブロックへの登録（配信管理サーバがプログラム本体を保持している場合）

図２５に示す動作例では、ユーザが配信を希望するプログラムの本体は配信管理サーバ１６Ａに格納されておらず、コンテンツサーバ１９に格納されていた。これに対し、図２６に示す動作例では、ユーザが配信を希望するプログラムの本体が配信管理サーバ１６Ａに記憶されている。以下、この図２６に示す動作例について説明する。

ユーザが配信管理サーバ１６Ａから受け取った登録リストを参照し、所望のプログラムを選択する操作を行うと、そのプログラムに対応した登録リスト内ポインタを含んだ配信要求が移動体端末１１から配信管理サーバ１６Ａのユーザ情報格納部５１に送られる（ステップＳ１６１）。

ユーザ情報格納部５１は、ユーザｋの移動体端末１１から配信要求を受け取ると、ユーザ個別情報格納部５３－ｋの実配信情報格納部５４の各領域のうち配信要求に含まれる登録リスト内ポインタに対応した領域から、配信要求の対象であるプログラムのＵＲＬまたはプログラム本体の格納先を特定するポインタデータを読み出す。そして、このポインタデータを含む配信要求をプログラム情報格納部５２に送る（ステップＳ１６２）。

プログラム情報格納部５２は、この配信要求中のポインタデータによって特定された領域を参照する。そして、当該領域にプログラム本体が格納されている場合、セキュア通信制御部６２は、認証サーバ１８に対して証明書要求、すなわち、そのプログラム本体を暗号化してユーザｋのＵＩＭ１２に送るのに必要なＵＩＭ公開鍵の要求を送る（ステップＳ１６３）。

認証サーバ１８は、配信要求に対応するプログラムがＵＩＭ１２への書き込みが許可されたプログラムである場合には、ＵＩＭ公開鍵をセキュア通信制御部６

２に送る（ステップＳ１６４）。

セキュア通信制御部６２は、このＵＩＭ公開鍵を受け取り、これが正規なものであると判断すると、配信対象であるプログラムをＵＩＭ公開鍵によって暗号化し、証明書付きプログラムを生成する。

移動体端末１１において、ユーザがプログラムの配信を許可する操作を行うと、配信管理サーバ１６Ａのセキュア通信制御部６２は、移動体端末１１のＵＩＭ１２に証明書付きプログラムを送る（ステップＳ１６５）。

ＵＩＭ１２は、ＵＩＭ公開鍵と対をなすＵＩＭ秘密鍵を記憶しており、このＵＩＭ秘密鍵を用いて、プログラムを復号する。そして、当該プログラムを基本ブロック４０－Ｘに書き込む。

以後の動作は図２５に示されたものと同様であり、図２６におけるステップＳ１６６～Ｓ１７１は、図２５におけるステップＳ１４８～Ｓ１５３に対応している。

［２．３．１．３］ＵＩＭの基本ブロックへの登録（配信管理サーバがプログラム本体を保持し、セキュア通信制御部がＵＩＭ公開鍵を保持している場合）

移動体端末１１から配信管理サーバ１６Ａに配信要求が送られたとき、配信管理サーバ１６Ａのセキュア通信制御部６２がプログラムの配信先であるＵＩＭ１２のＵＩＭ公開鍵を保持しているような場合が起こりうる。例えば短時間のうちに同一のＵＩＭ１２に対するプログラムの配信が行われるようなときにこのようなことが起こりうる。図２７はそのような場合における動作例を示している。この動作例においては、配信要求に対応したプログラム本体が見つかったとき、セキュア通信制御部６２に保持されたＵＩＭ公開鍵を用いてプログラムの暗号化が行われ、ＵＩＭ１２に書き込まれる。図２７に示す動作は、認証サーバ１８からＵＩＭ公開鍵を取得するステップＳ１６３およびＳ１６４に相当する動作が欠如している点を除き、図２６に示す動作と同様であり、図２７におけるステップＳ１８１、Ｓ１８２、Ｓ１８３～Ｓ１８９は、図２６におけるステップＳ１６１、Ｓ１６２、Ｓ１６５～Ｓ１７１に対応している。

［２．３．１．４］ＵＩＭのフリー基本ブロックへの登録

ユーザは、移動体端末１１を操作することによりＵＩＭ１２のフリー基本ブロック４０－Ｆ１にプログラムを登録することができる。図２８はその動作を示すものである。

ＵＩＭ１２のフリー基本ブロック４０－Ｆ１へのプログラムの登録を行う場合、ユーザは移動体端末１１を操作することにより所望のコンテンツサーバ１９Ｘにアクセスし、所望のプログラムの配信要求を送る（ステップＳ１９１）。

この配信要求を受け取ったコンテンツサーバ１９Ｘは、要求されたプログラムを配信管理サーバ１６Ａのセキュア通信制御部６２に配信する（ステップＳ１９２）。

ユーザがフリー基本ブロック４０－Ｆ１に対する配信を許可する操作を行い、その操作を示す情報が移動体端末１１から配信管理サーバ１６Ａに送られると、セキュア通信制御部６２は、移動体端末１１のＵＩＭ１２に対して、プログラムを配信する（ステップＳ１９３）。このプログラムは暗号化して送っても良く、暗号化しないで送ってもよい。ＵＩＭ１２は、このプログラムをフリー基本ブロック４０－Ｆ１に書き込む。

ＵＩＭ１２は，プログラムの書き込みが終了すると、その旨を示す書込終了通知を配信管理サーバ１６に送信する（ステップＳ１８４）。

配信管理サーバ１６のユーザ情報格納部５１は、ユーザｋのＵＩＭ１２から書込終了通知を受け取り、個別ユーザ情報格納部５３－ｋにおけるフリー基本ブロック４０－Ｆに対応した領域に記憶された配信回数などの情報を更新する（ステップＳ１９５）。

この更新が終わると、ユーザ情報格納部５１は、フリー基本ブロック４０－Ｆ１に書き込まれたプログラムについてのアクティベーション指示をＵＩＭ１２に送る（ステップＳ１９６）。

ＵＩＭ１２は、この指示に従って、プログラムのアクティベーションを終えると、フリー基本ブロック４０－Ｆ１内のプログラムのアクティベーションが終了した旨を示すアクティベーション応答通知を配信管理サーバ１６のユーザ情報格納部５１に送信する（ステップＳ１９７）。

ユーザ情報格納部５１は、ユーザｋのＵＩＭ１２からアクティベーション応答通知を受けると、個別ユーザ情報格納部５３－ｋにおけるフリー基本ブロック４０－Ｆに対応した領域にアクティベーションが完了した旨の情報を登録する。そして、ユーザ情報格納部５１は、移動体端末１１に対して登録完了の旨をプログラムリストとして通知して処理を終了する（ステップＳ１９８）。

［２．３．１．５］プログラムのユーザ情報格納部からの削除

次にユーザ情報格納部５１に登録されているプログラムを削除する場合の処理について図２９を参照して説明する。

ユーザは、所定の操作を行うことにより、配信管理サーバ１６Ａから受け取った登録プログラムリストをディスプレイ部２１に表示させることができる。この状態において、ユーザが所望のプログラムを特定して、配信管理サーバ１６Ａでのそのプログラムの削除を指示すると、削除対象を特定する情報を含むプログラム登録削除要求が配信管理サーバ１６Ａのユーザ情報格納部５１に送られる（ステップＳ２０１）。

ユーザ情報格納部５１は、削除対象であるプログラムがＵＩＭ１２の基本ブロック４０－１～４０－７のいずれかから既に削除されている場合には、そのプログラムの配信元であるコンテンツサーバ１９に、ユーザがプログラムの利用の解約を希望している旨の解約要求を送る（ステップＳ２０２）。なお、削除対象であるプログラムが削除されずにＵＩＭ１２の基本ブロック４０－１～４０－７のいずれかに残っている場合には、後述する基本ブロック４０－１～４０－７からのプログラムの削除処理が配信管理サーバ１６Ａの主導で同時に行われる。

コンテンツサーバ１９は、解約要求を受け取ると、解約許可通知を配信管理サーバ１６Ａのユーザ情報格納部５１に送る（ステップＳ２０３）。

ユーザ情報格納部５１は、解約許可通知を受け取ると、ステップＳ２０１において削除要求を受けたプログラムに関する情報を削除し、移動体端末１１に対して削除後の登録プログラムリストを移動体端末１１に送る（ステップＳ２０４）。

［２．３．１．６］プログラムのＵＩＭの基本ブロックからの削除

次にＵＩＭ１２の基本ブロック４０－１～４０－７からプログラムを削除する

場合の処理について図３０を参照して説明する。

ユーザは、所定の操作を行うことにより、既に移動体端末１１に送信されている登録プログラムリストをディスプレイ部２１に表示させることができる。この状態において、ユーザが所望のプログラムを特定してその削除を指示を行うと、ＵＩＭ１２の基本ブロック４０－１～４０－７のうち削除対象のプログラムが格納されている基本ブロックが求められ、この基本ブロックを特定する情報を含む削除要求が移動体端末１１から配信管理サーバ１６Ａのユーザ情報格納部５１に送信される（ステップＳ２１１）。

ユーザ情報格納部５１は、削除要求を受け取ると、ＵＩＭ１２に削除許可通知を送る（ステップＳ２１２）。

ＵＩＭ１２は、削除許可通知を受け取ると、ステップＳ２１１においてユーザによって特定されたプログラムを該当する基本ブロックから削除し、削除終了通知をユーザ情報格納部５１に送る（ステップＳ２１３）。

これによりユーザ情報格納部５１は、伝送制御部６１の制御下で対応するプログラムに関する情報を削除し、コンテンツサーバ１９に削除通知を行う（ステップＳ２１４）。

また、ユーザ情報格納部５１は、移動体端末１１に対して削除完了の旨をプログラムリストとして通知して処理を終了する。

［２．３．１．６．１］　基本ブロックからのプログラムの削除処理を配信管理サーバの主導で同時に行う場合

前述したように基本ブロック４０-1～４０-7 からのプログラムの削除処理を配信管理サーバ１６Ａの主導でプログラムのユーザ情報格納部５１からの削除と同時に行う場合には、配信管理サーバのユーザ情報格納部５１は、上述したステップＳ２１１及びステップＳ２１２の処理に代えて、ユーザ情報格納部５１が削除を要求するプログラムを特定して削除指示をＵＩＭに対して行うこととなる。

［２．３．１．７］ユーザ情報格納部の利用を禁止する場合

本実施形態では、ユーザ情報格納部５１をユーザ側から利用できなくするユーザ情報格納部ディアクティベーション処理を実行することが可能である。このユ

ーザ情報格納部ディアクティベーション処理は、配信管理サーバ１６Ａ側においてサービスの提供を一時的に停止したり、コンテンツサーバ１９を保有しているコンテンツプロバイダからの要請により当該ユーザに対する配信管理サーバ１６Ａのサービスを一次的に停止する場合などに行われる。このユーザ情報格納部ディアクティベーション処理が行われると、ユーザ情報格納部５１に登録されているプログラムのＵＩＭ１２への配信が禁止されたり、ＵＩＭ１２に登録されているプログラムの削除が禁止される、という効果が生じる。

以下、図３１を参照して、このユーザ情報格納部ディアクティベーション処理について説明する。なお、以下においては、コンテンツサーバ１９がユーザ情報格納部ディアクティベーション処理を要求する場合について説明する。

まず、コンテンツサーバ１９が配信管理サーバ１６Ａのユーザ情報格納部５１にユーザ情報格納部ディアクティベーション要求を送る（ステップＳ２２１）。

ユーザ情報格納部５１は、このユーザ情報格納部ディアクティベーション要求を受け取ると、利用禁止状態（ディアクティベーション状態）となるとともに、コンテンツサーバ１９にユーザ情報格納部ディアクティベーション許可通知を送る（ステップＳ２２２）。

続いて、ユーザ情報格納部５１は、ユーザ情報格納部５１の利用が禁止された旨のユーザ情報格納部ディアクティベーション通知を移動体端末１１に送る（ステップＳ２２３）。

これにより、移動体端末１１のユーザは、ユーザ情報格納部５１の利用が禁止された旨を把握することができる。

［２．３．１．７．１］ユーザ情報格納部ディアクティベーションを配信管理サーバが行う場合

ユーザ情報格納部ディアクティベーションを配信管理サーバ１６Ａ自身が行う場合には、ユーザ情報格納部５１は、利用禁止状態（ディアクティベーション状態）となり、ユーザ情報格納部５１の利用が禁止された旨のユーザ情報格納部ディアクティベーション通知を移動体端末１１に送る（ステップＳ２２３）。

［２．３．１．８］ＵＩＭの基本ブロックに格納されているプログラムの利用を

禁止する場合

次にＵＩＭ１２の基本ブロック４０－１～４０－７あるいはフリー基本ブロック４０－Ｆ１に格納されているプログラムの利用を禁止する基本ブロックディアクティベーション処理について図３２を参照して説明する。

この処理は、移動体端末１１が盗難にあった場合やコンテンツプロバイダから当該ユーザに対する利用を禁止する依頼があった場合に行われる。この処理が行われると、処理対象となった基本ブロック（フリー基本ブロックも含む。）に格納されているプログラムのユーザによる利用が禁止される。なお、以下においては、移動体端末１１の盗難時の対応などのユーザサービスを行うユーザサービスサーバ６５がユーザからの通報に基づいて基本ブロックディアクティベーション処理を要求する場合について説明する。

図３２に基本ブロックディアクティベーション処理のシーケンスを示す。

まず、ユーザサービスサーバ６５が配信管理サーバ１６Ａのユーザ情報格納部５１に基本ブロックディアクティベーション要求を送る（ステップＳ２３１）。

ユーザ情報格納部５１は、この基本ブロックディアクティベーション要求を受け取ると、ＵＩＭ１２にディアクティベーション指示を送る（ステップＳ２３２）。

これによりＵＩＭ１２は、基本ブロックディアクティベーション要求に対応する基本ブロックをディアクティベーション状態とし、ＵＩＭ１２は、基本ブロックの利用が禁止された旨を基本ブロックディアクティベーション応答として通知する（ステップＳ２３３）。

続いて、ユーザ情報格納部５１は、ユーザサービスサーバ６５に対してＵＩＭ１２の基本ブロックの利用が禁止された旨を基本ブロックディアクティベーション終了通知として通知する（ステップＳ２３４）。

さらにユーザ情報格納部５１は、移動体端末１１に対して基本ブロック（フリー基本ブロックを含む場合もある。）の利用が禁止された旨をユーザ情報格納部リストとして通知して処理を終了する（ステップＳ２３５）。

［２．４］第２実施形態の効果

以上の説明のように、第２実施形態によれば、記憶モジュール（ＵＩＭ）の記

憶領域の数の制限を越えてプログラムを配信することが可能となり、ユーザの使い勝手を向上することができる。

また、配信管理サーバにおいて配信しているプログラムの活性化／不活性化および削除、配信可能状態にあるプログラムの配信および活性化／不活性化および削除を容易に管理することができる。

[３] 実施形態の変形例

[３．１] 第１変形例

以上の説明においては、配信管理サーバが一つの場合について説明したが、配信管理サーバを複数設け、分散処理を行うように構成することが可能である。

この場合には、各ＵＩＭに格納されているプログラムや、各プログラムの格納領域に関する情報は、共用のデータベースに格納しておくようにすればよい。

[３．２] 第２変形例

以上の説明においては、配信管理サーバが直接回線交換網に接続されている場合について説明したが、パケット交換網を構成するインターネットおよびインターネットゲートウェイ装置を介して回線交換網と接続するように構成することも可能である。

[３．３] 第３変形例

以上の説明においては、記憶モジュールとしてＵＩＭの場合についてのみ説明したが、各種のＩＣカードメモリについて適用することも可能である。この場合に、記憶モジュールの設置は移動体端末に限ることなく、固定端末であっても適用が可能である。

請求の範囲

1．プログラムの配信要求を送信する手段を有する移動体端末と、

前記移動体端末に内蔵あるいは接続された記憶モジュールと、

前記配信要求を受信し、配信対象であるプログラムを送信するコンテンツサーバと、

前記コンテンツサーバから前記プログラムを受信し、前記コンテンツサーバが予め許可されたコンテンツサーバである場合に限り、前記コンテンツサーバから受信したプログラムを前記移動体端末に内蔵あるいは接続された記憶モジュールに送信する配信管理サーバとを具備し、

前記記憶モジュールは、

記憶部と、

前記移動体端末を介して前記配信管理サーバから受信されたプログラムを前記記憶部に記憶し、要求に応じて、前記記憶部に記憶されたプログラムを実行する制御部と

を具備することを特徴とするプログラム配信システム。

2．前記記憶モジュールに固有の第1の暗号鍵を格納する認証サーバをさらに具備し、

前記記憶モジュールの制御部は、前記第1の暗号鍵により暗号化されたプログラムを復号化し、この復号化に成功した場合に限り、復号化により得られたプログラムを前記記憶部に格納するものであり、

前記コンテンツサーバは、前記配信要求を受信したとき、前記第1の暗号鍵を前記認証サーバから取得し、これを用いて配信対象であるプログラムを暗号化し、さらに予め取得した第2の暗号鍵を用いて暗号化し、前記配信管理サーバに送信し、

前記配信管理サーバは、前記コンテンツサーバから受信した暗号化されたプログラムを前記第2の暗号鍵を用いて復号化して、前記第1の暗号鍵のみによって

暗号化されたプログラムを生成し、前記復号化に成功した場合に限り、前記復号化によって得られたプログラムを前記記憶モジュールに送信することを特徴とする請求項１に記載のプログラム配信システム。

３．前記記憶モジュールは、プログラムとともに当該プログラムによって使用されるデータを記憶することを特徴とする請求項１に記載のプログラム配信システム。

４．前記配信管理サーバは、前記記憶モジュールにプログラムを配信した時点で課金処理を開始する課金処理部を備えたことを特徴とする請求項１に記載のプログラム配信システム。

５．前記課金処理部は、前記記憶モジュールの貸与料についての課金を行うことを特徴とする請求項４に記載のプログラム配信システム。

６．前記配信管理サーバは、前記記憶モジュールのためのプログラムを保持した時点で課金処理を開始する課金処理部を具備することを特徴とする請求項１に記載のプログラム配信システム。

７．前記課金処理部は、前記記憶モジュールの貸与料についての課金を行うことを特徴とする請求項６に記載のプログラム配信システム。

８．前記配信管理サーバは、他の装置からの要求によりアクティベーション指示を前記記憶モジュールに送信し、

前記記憶モジュールは、前記アクティベーション指示を受信したとき、前記記憶モジュールに記憶されており、前記アクティベーション指示によって指示されたプログラムを実行可能な状態にすることを特徴とする請求項１に記載のプログラム配信システム。

９．前記配信管理サーバは、他の装置からの要求によりディアクティベーション指示を前記記憶モジュールに送信し、

前記記憶モジュールは、前記ディアクティベーション指示を受信したとき、前記記憶モジュールに記憶されており、前記ディアクティベーション指示によって指示されたプログラムを実行不能な状態にすることを特徴とする請求項１に記載のプログラム配信システム。

１０．前記配信管理サーバは、他の装置からの要求により削除指示を前記記憶モジュールに送信し、

前記記憶モジュールは、前記削除指示を受信したとき、前記記憶モジュールから前記削除指示によって指示されたプログラムを削除することを特徴とする請求項１に記載のプログラム配信システム。

１１．前記配信管理サーバは、前記記憶モジュール宛てに送った情報に基づいて、前記記憶モジュール内におけるプログラムの状態を管理する手段を具備することを特徴とする請求項１に記載のプログラム配信システム。

１２．前記配信管理サーバは、前記記憶モジュールに関するバージョン情報を取得し、該バージョン情報に基づいて前記プログラムの配信を行うか否かを判断することを特徴とする請求項１に記載のプログラム配信システム。

１３．前記移動体端末は、移動通信網を利用した通信を行うための第１の通信部と、

この第１の通信部とは異なる第２の通信部とを具備し、

前記記憶モジュールの制御部は、前記記憶モジュールに記憶されたプログラムに従って前記第２の通信部を利用した通信を行う手段を具備することを特徴とする請求項１に記載のプログラム配信システム。

１４．プログラムの配信要求を送信する手段を有する移動体端末と、

前記移動体端末に内蔵あるいは接続された記憶モジュールと、

前記配信要求を受信し、配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムである場合に、該プログラムを取得して前記移動体端末に内蔵あるいは接続された記憶モジュール宛てに送信する配信管理サーバとを具備し、

前記記憶モジュールは、

記憶部と、

前記移動体端末を介して情報を受信し、該情報が前記配信管理サーバから受信されたプログラムである場合に限って前記記憶部に記憶し、要求に応じて、前記記憶部に記憶されたプログラムを実行する制御部と

を具備することを特徴とするプログラム配信システム。

１５．前記配信管理サーバは、前記記憶モジュールに送られたプログラムを特定するポインタデータを記憶する実配信情報記憶部を具備することを特徴とする請求項１４に記載のプログラム配信システム。

１６．前記記憶モジュールの記憶部は、プログラムを格納するための複数の基本ブロックを有し、前記配信管理サーバの実配信情報記憶部は、前記複数の基本ブロックに対応した複数の領域を具備することを特徴とする請求項１５に記載のプログラム配信システム。

１７．前記配信管理サーバは、前記記憶モジュールへの配信が可能であるが現在は前記記憶モジュールに記憶されていないプログラムを特定するポインタデータを記憶する仮想配信情報記憶部を具備し、前記仮想配信情報記憶部に記憶されたポインタデータによって特定されたプログラムの前記記憶モジュールへの配信が要求されたとき、当該プログラムを前記記憶モジュールに配信するとともに、当

該プログラムを特定するポインタデータを前記仮想情報配信記憶部から前記実配信情報記憶部に移動させることを特徴とする請求項１６に記載のプログラム配信システム。

１８．前記配信管理サーバは、前記コンテンツサーバから取得可能なプログラムの所在を示すアドレス情報または前記コンテンツサーバから取得したプログラムを記憶するプログラム情報記憶部を具備し、前記実配信情報記憶部または仮想配信情報記憶部に記憶されたポインタデータによって特定されたプログラムの前記記憶モジュールへの配信が要求されたとき、当該プログラムを前記プログラム情報記憶部を利用して取得し、前記記憶モジュールに配信することを特徴とする請求項１６に記載のプログラム配信システム。

１９．前記移動体端末は、メニューリスト要求を送信する手段を具備し、

前記配信管理サーバは、前記メニューリスト要求に応じて、前記移動体端末に内蔵または接続された記憶モジュールのために前記実配信情報記憶部および前記仮想配信情報記憶部に記憶されたポインタデータを参照し、該ポインタデータによって特定されるプログラムのリストを生成し、前記移動体端末に送信することと特徴とする請求項１７に記載のプログラム配信システム。

２０．前記移動体端末は、移動通信網を利用した通信を行うための第１の通信部と、

この第１の通信部とは異なる第２の通信部とを具備し、

前記記憶モジュールの制御部は、前記記憶モジュールに記憶されたプログラムに従って前記第２の通信部を利用した通信を行う手段を具備することを特徴とする請求項１４に記載のプログラム配信システム。

２１．配信先に固有の第１の暗号鍵による暗号化と、プログラム配信が許可されたコンテンツサーバに固有の第２の暗号鍵による暗号化とを経たプログラムを前

記コンテンツサーバから受信する手段と、

前記コンテンツサーバから受信されたプログラムを前記第２の暗号鍵による暗号化が施される前の状態に戻す復号化を行うことにより、前記第１の暗号鍵のみにより暗号化されたプログラムを生成し、移動体端末に内蔵または接続された記憶モジュールに配信する手段と

を具備することを特徴とする配信管理サーバ。

２２．許可されたコンテンツサーバから予め取得されたプログラムまたはそのアドレス情報を記憶するプログラム情報格納部と、

移動体端末に内蔵または接続された記憶モジュールに格納されているプログラムと同一のプログラムまたはそのアドレス情報が前記プログラム情報格納部に格納されている場合に該プログラムまたはそのアドレス情報の前記プログラム情報格納部における格納位置を示すポインタデータを記憶する実配信情報記憶部と、

前記記憶モジュールに配信可能ではあるが前記記憶モジュールに現在格納されていないプログラムと同一のプログラムまたはそのアドレス情報が前記プログラム情報格納部に格納されている場合に該プログラムの前記プログラム情報格納部における格納位置を示すポインタデータを記憶する仮想配信情報記憶部と、

前記移動体端末からの要求に応じて、前記仮想配信情報記憶部に記憶されたポインタデータによって特定されるプログラムを前記プログラム情報格納部を利用して取得して前記記憶モジュール宛てに配信し、該ポインタデータを前記実配信情報格納部に移動させる手段と

を具備することを特徴とする配信管理サーバ。

２３．記憶モジュールが内蔵あるいは接続された移動体端末からプログラムの配信要求を受けたとき、前記記憶モジュールに固有の暗号鍵を外部の認証サーバから取得する手段と、

前記第１の暗号鍵により配信対象であるプログラムを暗号化する第１の暗号化手段と、

第１の暗号化手段により得られたプログラムに対し、前記記憶モジュールへのプログラムの配信を行う配信管理サーバが復号化可能な暗号化を施す第２の暗号化手段と、

前記第１および第２の暗号化手段による暗号化を経たプログラムを前記配信管理サーバに送信する手段と

を具備することを特徴とするコンテンツサーバ。

２４．移動体端末に内蔵または接続される記憶モジュールにおいて、

記憶部と、

暗号化されたプログラムを前記移動体端末を介して特定の配信管理サーバから受信し、予め記憶された秘密鍵によりプログラムの復号化を行い、この復号化が成功した場合に限って該プログラムを前記記憶部に記憶し、要求に応じて、前記記憶部に記憶されたプログラムを実行する制御部と

を具備することを特徴とする記憶モジュール。

２５．前記記憶部は、プログラムを実行するための複数の記憶ブロックと、各記憶ブロックに記憶されたプログラムが実行可能か否かを示す活性化フラグを記憶する記憶領域を具備し、

前記制御部は、前記移動体端末を介して配信管理サーバから受信される指令に従って前記活性化フラグの書き込みを行い、前記移動体端末を介していずれか１の基本ブロックに格納されたプログラムの実行が指示された場合に、当該基本ブロックに対応した活性化フラグに基づいて実行指示に従うか拒否するかを決定することを特徴とする請求項２４に記載の記憶モジュール。

２６．記憶モジュールが内蔵あるいは接続された移動体端末がプログラムの配信要求をコンテンツサーバに送信する過程と、

前記コンテンツサーバが前記配信要求を受信し、配信対象であるプログラムを配信管理サーバに送信する過程と、

前記プログラムの送信元である前記コンテンツサーバが予め許可されたコンテンツサーバである場合に、前記配信要求を送信した移動体端末に内蔵あるいは接続された記憶モジュールに前記プログラムを送信する過程と

を具備することを特徴とするプログラム配信方法。

２７．記憶モジュールが内蔵あるいは接続された移動体端末がプログラムの配信要求をコンテンツサーバに送信する過程と、

前記コンテンツサーバが前記配信要求を受信し、前記記憶モジュールに固有の第１の暗号鍵を認証サーバから取得する過程と、

前記コンテンツサーバが配信対象であるプログラムを前記第１の暗号鍵により暗号化する過程と、

前記コンテンツサーバが前記第１の暗号鍵による暗号化を経たプログラムを予め取得した第２の暗号鍵により暗号化する過程と、

前記コンテンツサーバが前記第１の暗号鍵による暗号化と第２の暗号鍵による暗号化を経たプログラムを配信管理サーバに送信する過程と、

前記配信管理サーバが、前記コンテンツサーバから送信されたプログラムに対し、前記第２の暗号化を経る前の状態に戻す復号化を施して、前記第１の暗号鍵による暗号化のみを経たプログラムを生成する過程と、

前記配信管理サーバが、前記配信要求を送信した移動体端末に内蔵あるいは接続された記憶モジュールに前記第１の暗号鍵による暗号化のみを経たプログラムを送信する過程と

を具備することを特徴とするプログラム配信方法。

２８．記憶モジュールが内蔵あるいは接続された移動体端末が配信管理サーバにプログラムの配信要求を送信する過程と、

前記配信管理サーバが前記配信要求を受信し、配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムであるか否かを判断する過程と、

前記配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムである場合に、該プログラムを取得して前記移動体端末に内蔵あるいは接続された記憶モジュール宛てに送信する過程と

を具備することを特徴とするプログラム配信方法。

２９．前記配信管理サーバが前記記憶モジュールに代わってプログラムまたはそのアドレス情報を記憶手段に記憶する過程と、

前記配信管理サーバが、前記移動体端末のプログラムの配信要求を受けたとき、前記記憶手段を利用して、要求されたプログラムを取得し、前記記憶モジュールに配信する過程と

を具備することを特徴とする請求項２８に記載のプログラム配信方法。

３０．配信先に固有の第１の暗号鍵による暗号化と、プログラム配信が許可されたコンテンツサーバに固有の第２の暗号鍵による暗号化とを経たプログラムを前記コンテンツサーバから受信する処理と、

前記コンテンツサーバから受信されたプログラムを前記第２の暗号鍵による暗号化が施される前の状態に戻す復号化を行うことにより、前記第１の暗号鍵のみにより暗号化されたプログラムを生成し、移動体端末に内蔵または接続された記憶モジュールに配信する処理と

を配信管理サーバのコンピュータに実行させるプログラム。

３１．記憶モジュールが内蔵あるいは接続された移動体端末からプログラムの配信要求を受信する過程と、

配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムであるか否かを判断する過程と、

前記配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムである場合に、該プログラムを取得して前記移動体端末に内蔵あるいは接続された記憶モジュール宛てに送信する過程と

を配信管理サーバのコンピュータに実行させるプログラム。

３２．前記記憶モジュールに代わってプログラムまたはそのアドレス情報を記憶手段に記憶する過程と、

前記移動体端末のプログラムの配信要求を受けたとき、前記記憶手段を利用して、要求されたプログラムを取得し、前記記憶モジュールに配信する過程と

を具備することを特徴とする請求項３０に記載のプログラム配信方法。

３３．記憶モジュールが内蔵あるいは接続された移動体端末からプログラムの配信要求を受けたとき、前記記憶モジュールに固有の暗号鍵を外部の認証サーバから取得する処理と、

前記第１の暗号鍵により配信対象であるプログラムを暗号化する第１の暗号化処理と、

第１の暗号化処理により得られたプログラムに対し、前記記憶モジュールへのプログラムの配信を行う配信管理サーバが復号化可能な暗号化を施す第２の暗号化処理と、

前記第１および第２の暗号化処理による暗号化を経たプログラムを前記配信管理サーバに送信する処理と

をコンテンツサーバのコンピュータに実行させるプログラム。

３４．暗号化されたプログラムを移動体端末を介して特定の配信管理サーバから受信する処理と、

予め記憶された秘密鍵により、受信されたプログラムの復号化を行い、この復号化が成功した場合に限って該プログラムを記憶部に格納する処理と、

要求に応じて、前記記憶部に記憶されたプログラムを実行する処理と

を移動体端末に内蔵または接続される記憶モジュールの制御部に実行させるプログラム。

３５．配信先に固有の第１の暗号鍵による暗号化と、プログラム配信が許可されたコンテンツサーバに固有の第２の暗号鍵による暗号化とを経たプログラムを前記コンテンツサーバから受信する処理と、

前記コンテンツサーバから受信されたプログラムを前記第２の暗号鍵による暗号化が施される前の状態に戻す復号化を行うことにより、前記第１の暗号鍵のみにより暗号化されたプログラムを生成し、移動体端末に内蔵または接続された記憶モジュールに配信する処理と

を配信管理サーバのコンピュータに実行させるプログラム。

３６．記憶モジュールが内蔵あるいは接続された移動体端末からプログラムの配信要求を受信する過程と、

配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムであるか否かを判断する過程と、

前記配信対象であるプログラムが予め許可されたコンテンツサーバによって提供されているプログラムである場合に、該プログラムを取得して前記移動体端末に内蔵あるいは接続された記憶モジュール宛てに送信する過程と

を配信管理サーバのコンピュータに実行させるプログラム。

３７．前記記憶モジュールに代わってプログラムまたはそのアドレス情報を記憶手段に記憶する過程と、

前記移動体端末のプログラムの配信要求を受けたとき、前記記憶手段を利用して、要求されたプログラムを取得し、前記記憶モジュールに配信する過程と

を具備することを特徴とする請求項３６に記載のプログラム配信方法。

３８．記憶モジュールが内蔵あるいは接続された移動体端末からプログラムの配信要求を受けたとき、前記記憶モジュールに固有の暗号鍵を外部の認証サーバから取得する処理と、

前記第１の暗号鍵により配信対象であるプログラムを暗号化する第１の暗号化

処理と、

第１の暗号化処理により得られたプログラムに対し、前記記憶モジュールへのプログラムの配信を行う配信管理サーバが復号化可能な暗号化を施す第２の暗号化処理と、

前記第１および第２の暗号化処理による暗号化を経たプログラムを前記配信管理サーバに送信する処理と

をコンテンツサーバのコンピュータに実行させるプログラム。

３９．暗号化されたプログラムを移動体端末を介して特定の配信管理サーバから受信する処理と、

予め記憶された秘密鍵により、受信されたプログラムの復号化を行い、この復号化が成功した場合に限って該プログラムを記憶部に格納する処理と、

要求に応じて、前記記憶部に記憶されたプログラムを実行する処理と

を移動体端末に内蔵または接続される記憶モジュールの制御部に実行させるプログラム。

図 1

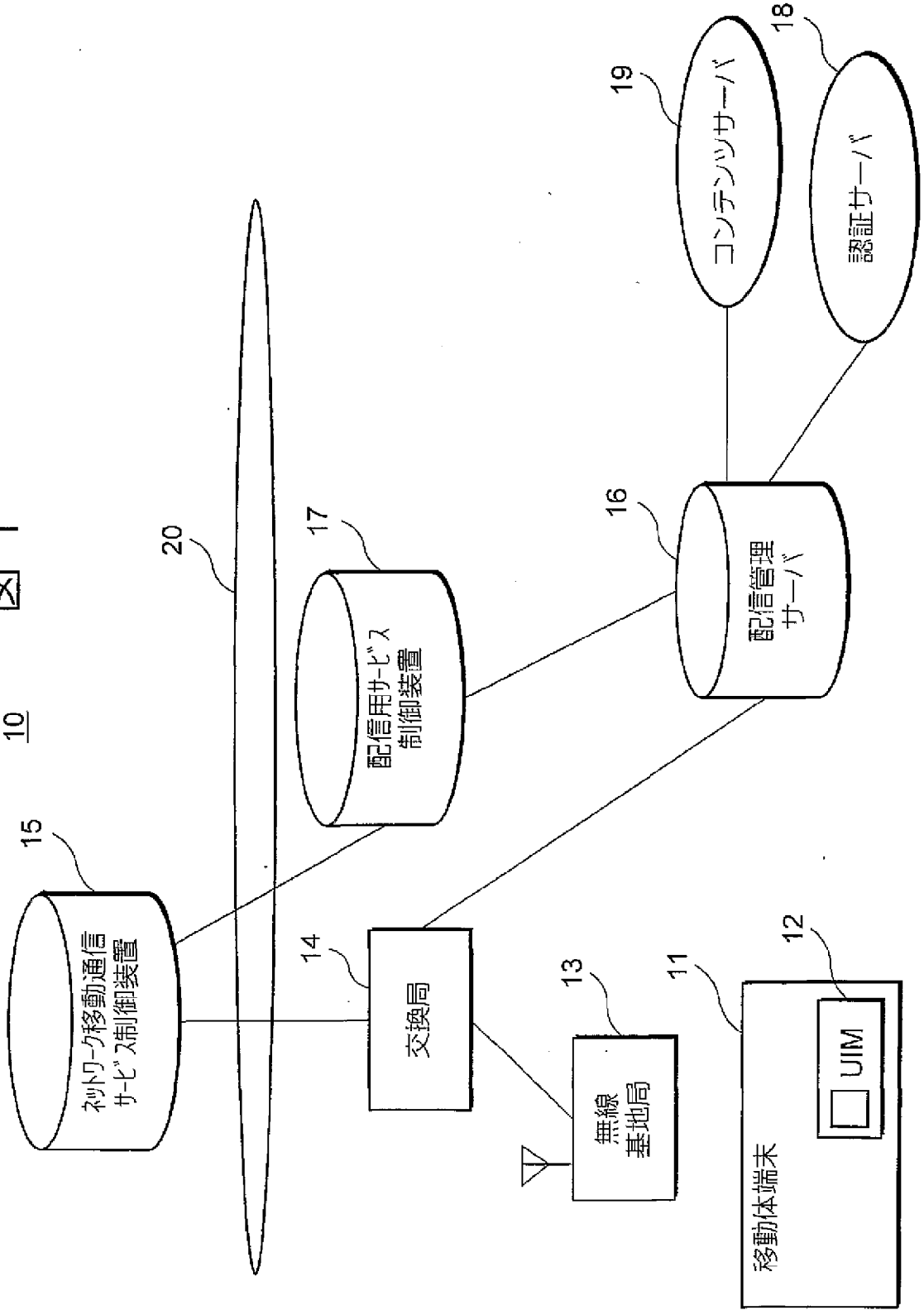

10
15
ネットワーク移動通信
サービス制御装置
20
17
配信用サービス
制御装置
16
配信管理
サーバ
19
コンテンツサーバ
18
認証サーバ
14
交換局
13
無線
基地局
11
移動体端末
12
UIM

図 2

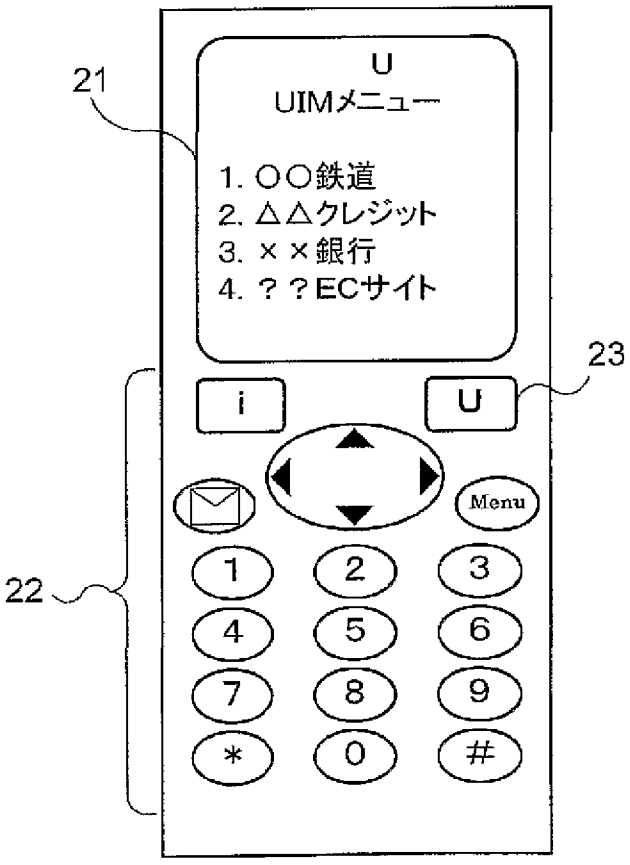

11
21
U
UIMメニュー
1. ○○鉄道
2. △△クレジット
3. ××銀行
4. ？？ECサイト
23
i
U
Menu
22
1
2
3
4
5
6
7
8
9
*
0
#

図 3

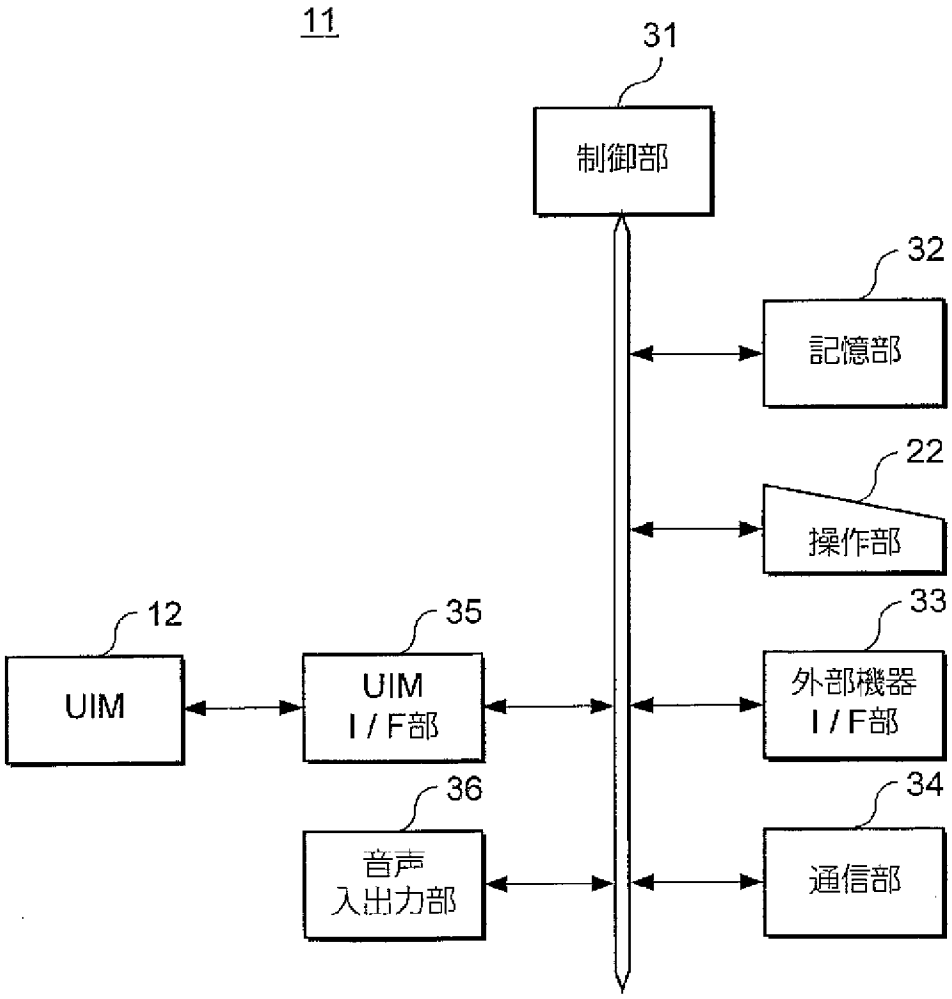

11
31
制御部
32
記憶部
22
操作部
33
外部機器
I / F部
34
通信部
12
UIM
35
UIM
I / F部
36
音声
入出力部

図 4

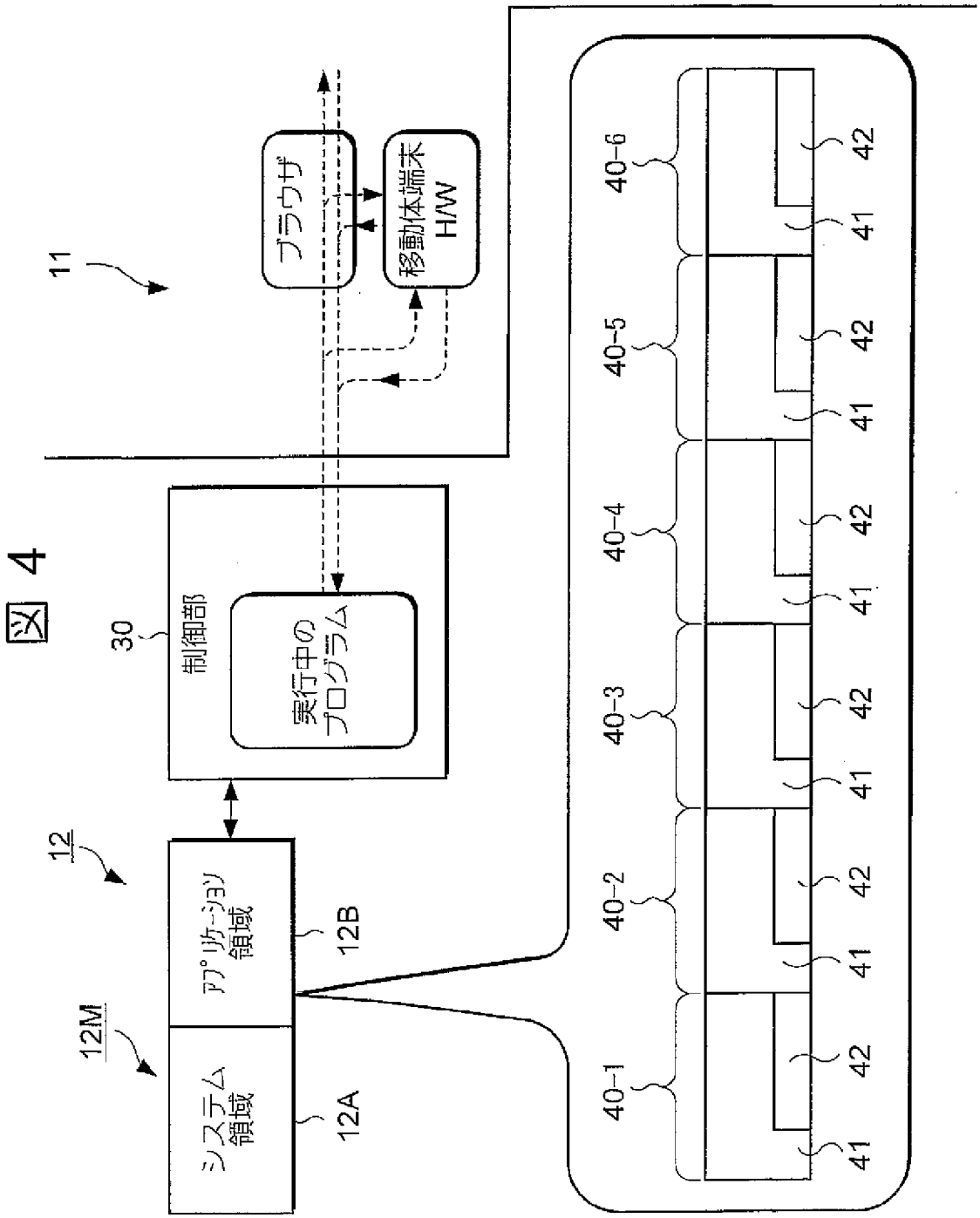

11
ブラウザ
移動体端末
H/W
30
制御部
実行中の
プログラム
12
12M
システム
領域
12A
ｱﾌﾟﾘｹｰｼｮﾝ
領域
12B
40-1
40-2
40-3
40-4
40-5
40-6
41
42

図 5

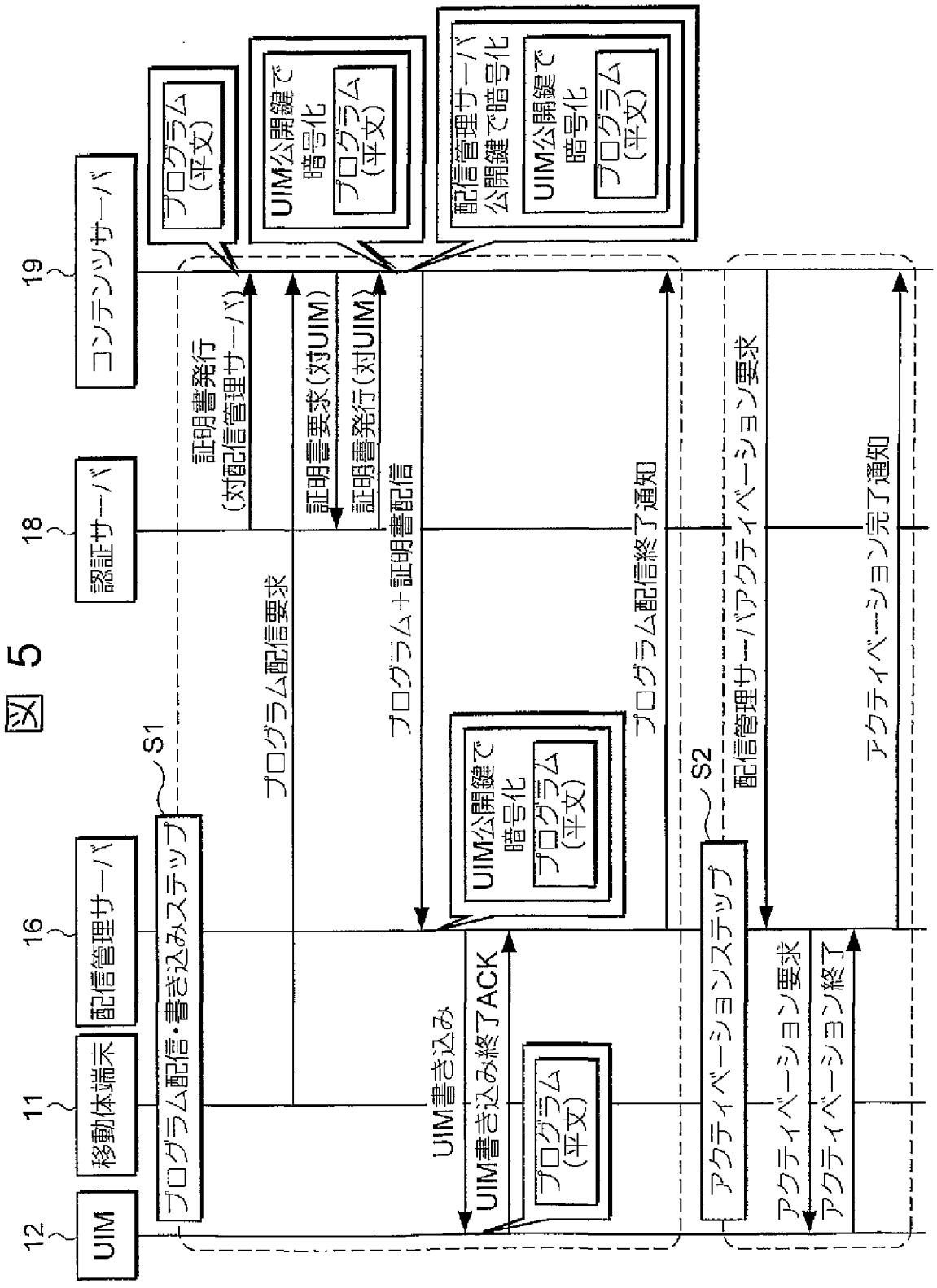

12
UIM
11
移動体端末
16
配信管理サーバ
18
認証サーバ
19
コンテンツサーバ
プログラム配信・書き込みステップ
S1
証明書発行
(対配信管理サーバ)
プログラム配信要求
証明書要求(対UIM)
証明書発行(対UIM)
プログラム＋証明書配信
プログラム
(平文)
UIM公開鍵で
暗号化
プログラム
(平文)
配信管理サーバ
公開鍵で暗号化
UIM公開鍵で
暗号化
プログラム
(平文)
UIM公開鍵で
暗号化
プログラム
(平文)
UIM書き込み
UIM書き込み終了ACK
プログラム
(平文)
プログラム配信終了通知
S2
アクティベーションステップ
配信管理サーバアクティベーション要求
アクティベーション要求
アクティベーション終了
アクティベーション完了通知

図 6

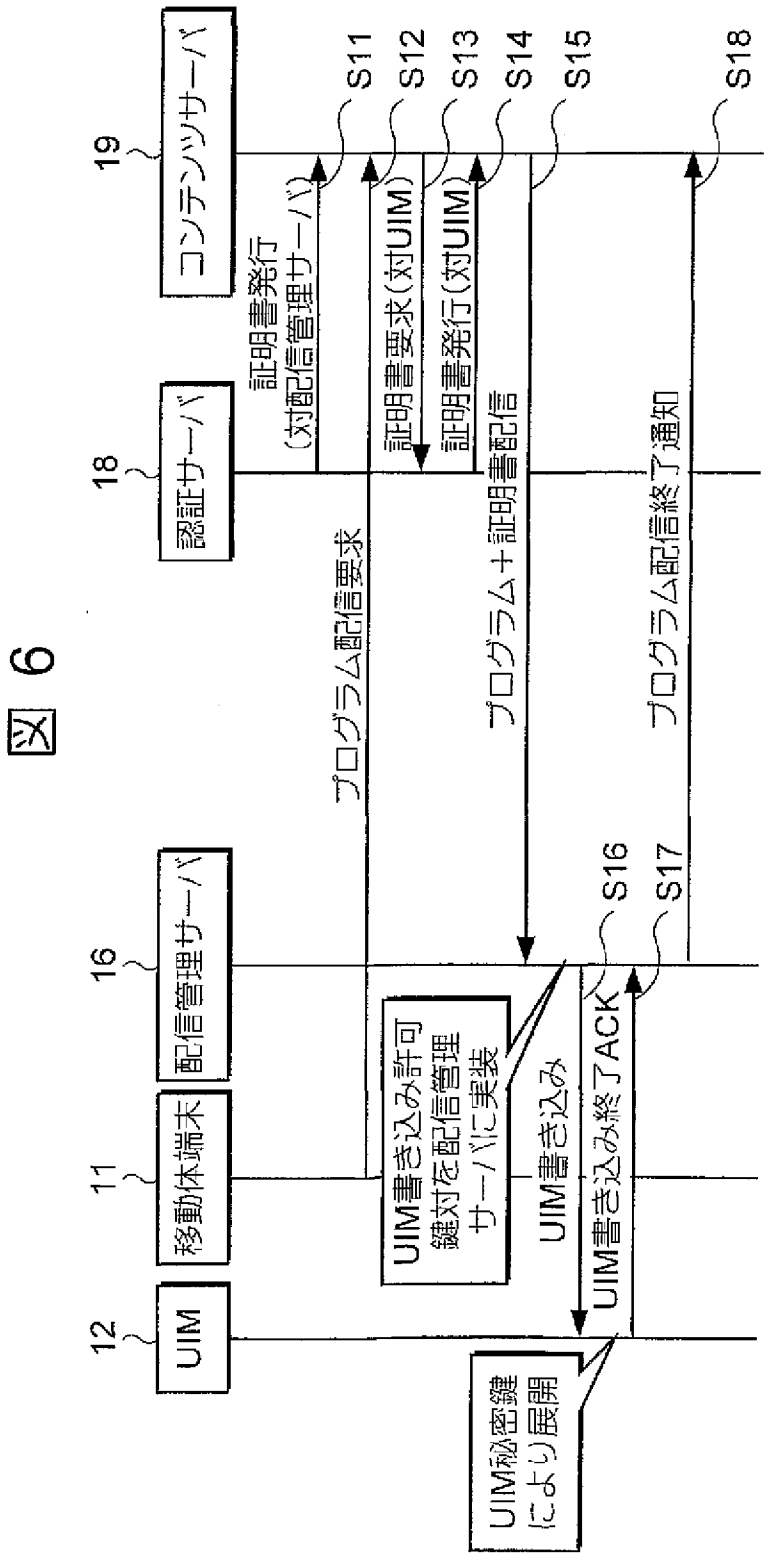

12
UIM
11
移動体端末
16
配信管理サーバ
18
認証サーバ
19
コンテンツサーバ
S11
S12
S13
S14
S15
S16
S17
S18
証明書発行
(対配信管理サーバ)
プログラム配信要求
証明書要求(対UIM)
証明書発行(対UIM)
プログラム＋証明書配信
プログラム配信終了通知
UIM書き込み許可
鍵対を配信管理
サーバに実装
UIM書き込み
UIM書き込み終了ACK
UIM秘密鍵
により展開

図 7

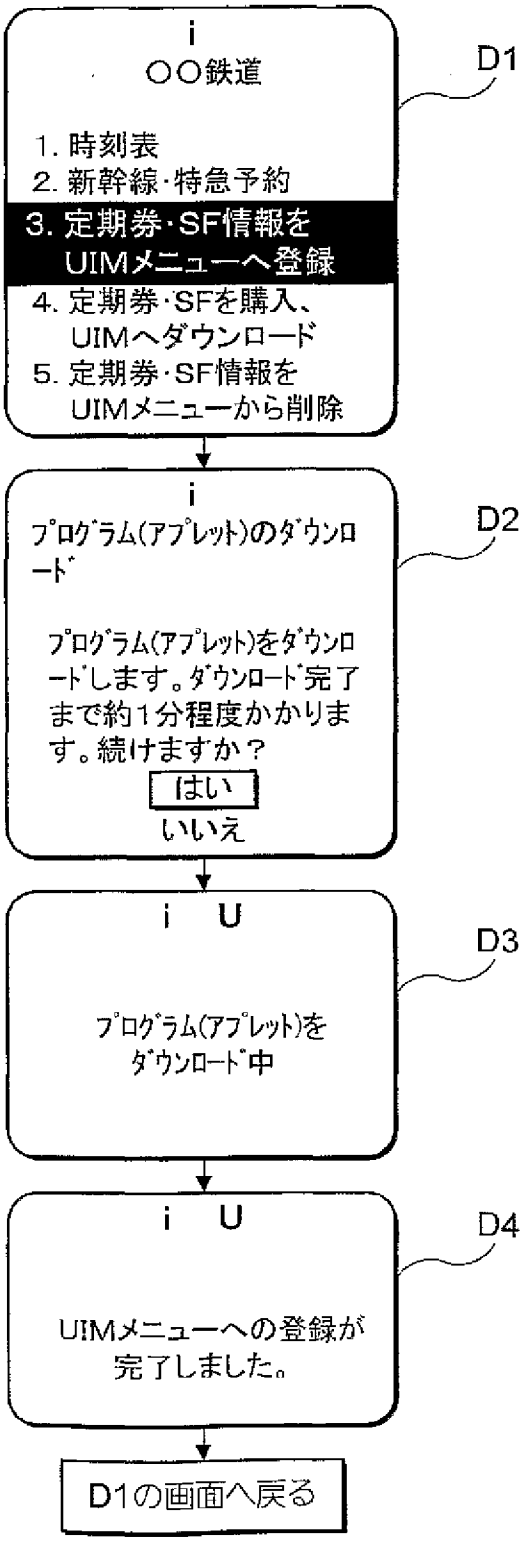

i
○○鉄道
1. 時刻表
2. 新幹線・特急予約
3. 定期券・SF情報を
UIMメニューへ登録
4. 定期券・SFを購入、
UIMへダウンロード
5. 定期券・SF情報を
UIMメニューから削除
D1
i
ﾌﾟﾛｸﾞﾗﾑ(ｱﾌﾟﾚｯﾄ)のﾀﾞｳﾝﾛｰﾄﾞ
ﾌﾟﾛｸﾞﾗﾑ(ｱﾌﾟﾚｯﾄ)をﾀﾞｳﾝﾛｰﾄﾞします。ﾀﾞｳﾝﾛｰﾄﾞ完了まで約1分程度かかります。続けますか？
はい
いいえ
D2
i U
ﾌﾟﾛｸﾞﾗﾑ(ｱﾌﾟﾚｯﾄ)を
ﾀﾞｳﾝﾛｰﾄﾞ中
D3
i U
UIMメニューへの登録が
完了しました。
D4
D1の画面へ戻る

図 8

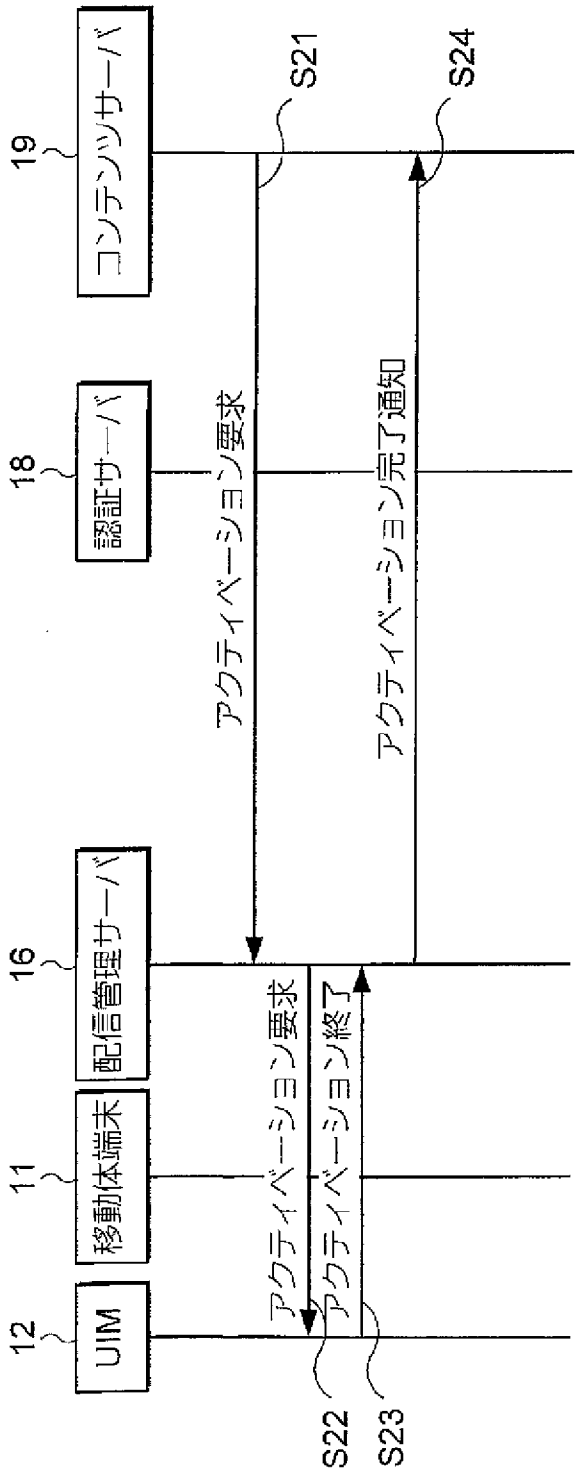

19
コンテンツサーバ
18
認証サーバ
16
配信管理サーバ
11
移動体端末
12
UIM
S21
S24
アクティベーション要求
アクティベーション完了通知
アクティベーション要求
アクティベーション終了
S22
S23

図 9

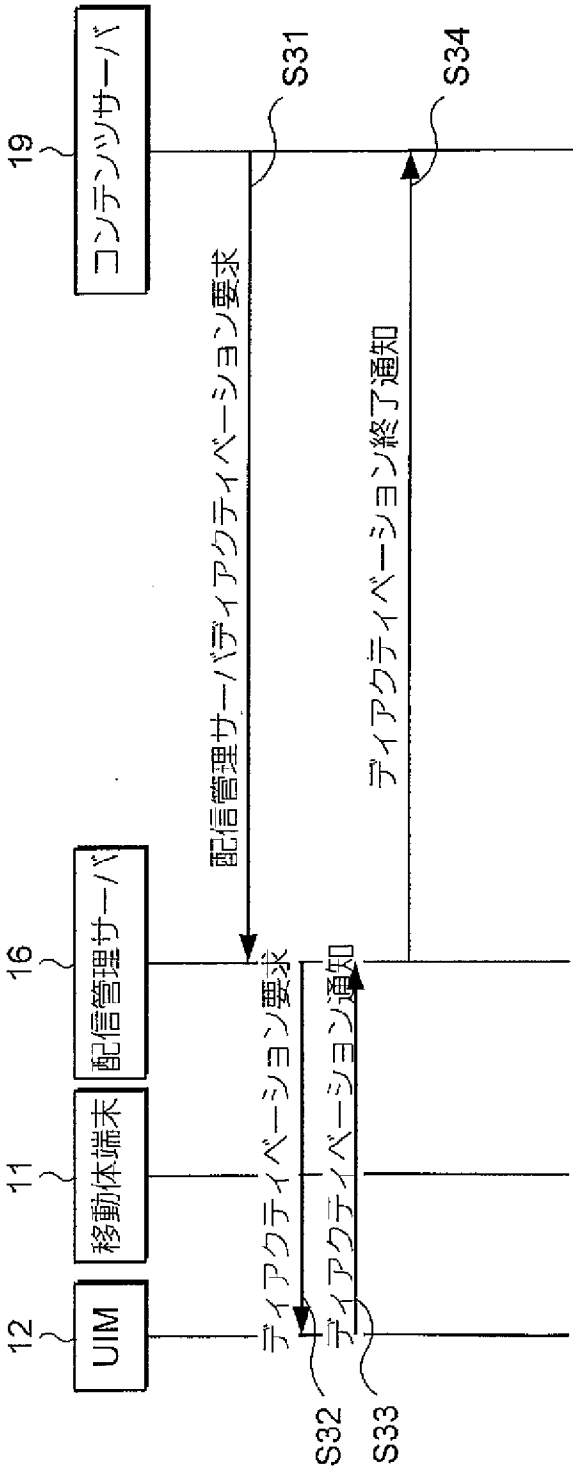

19
コンテンツサーバ
S31
S34
配信管理サーバディアクティベーション要求
ディアクティベーション終了通知
16
配信管理サーバ
11
移動体端末
12
UIM
ディアクティベーション要求
ディアクティベーション通知
S32
S33

図 10

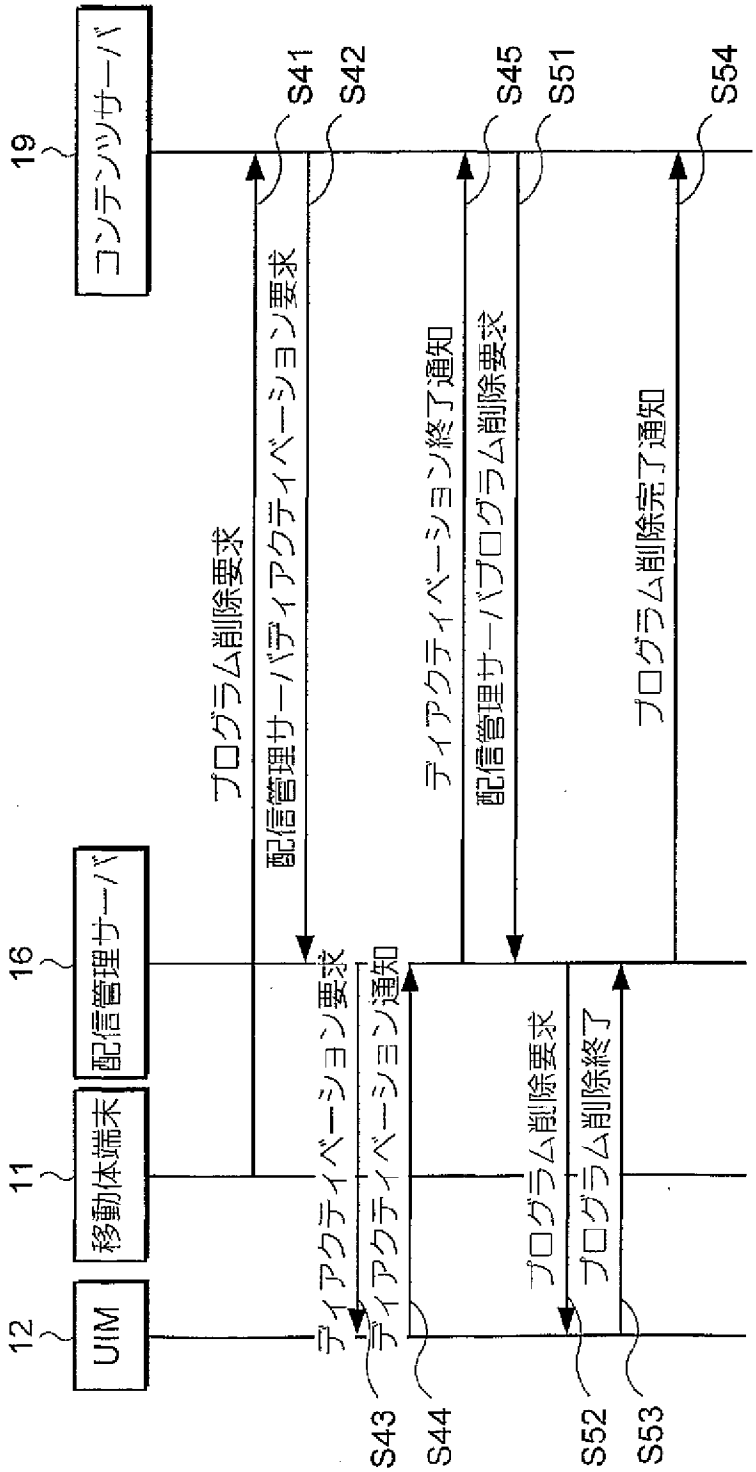

19
コンテンツサーバ
16
配信管理サーバ
11
移動体端末
12
UIM
プログラム削除要求
配信管理サーバディアクティベーション要求
ディアクティベーション要求
ディアクティベーション通知
ディアクティベーション終了通知
配信管理サーバプログラム削除要求
プログラム削除要求
プログラム削除終了
プログラム削除完了通知
S41
S42
S43
S44
S45
S51
S52
S53
S54

図 11

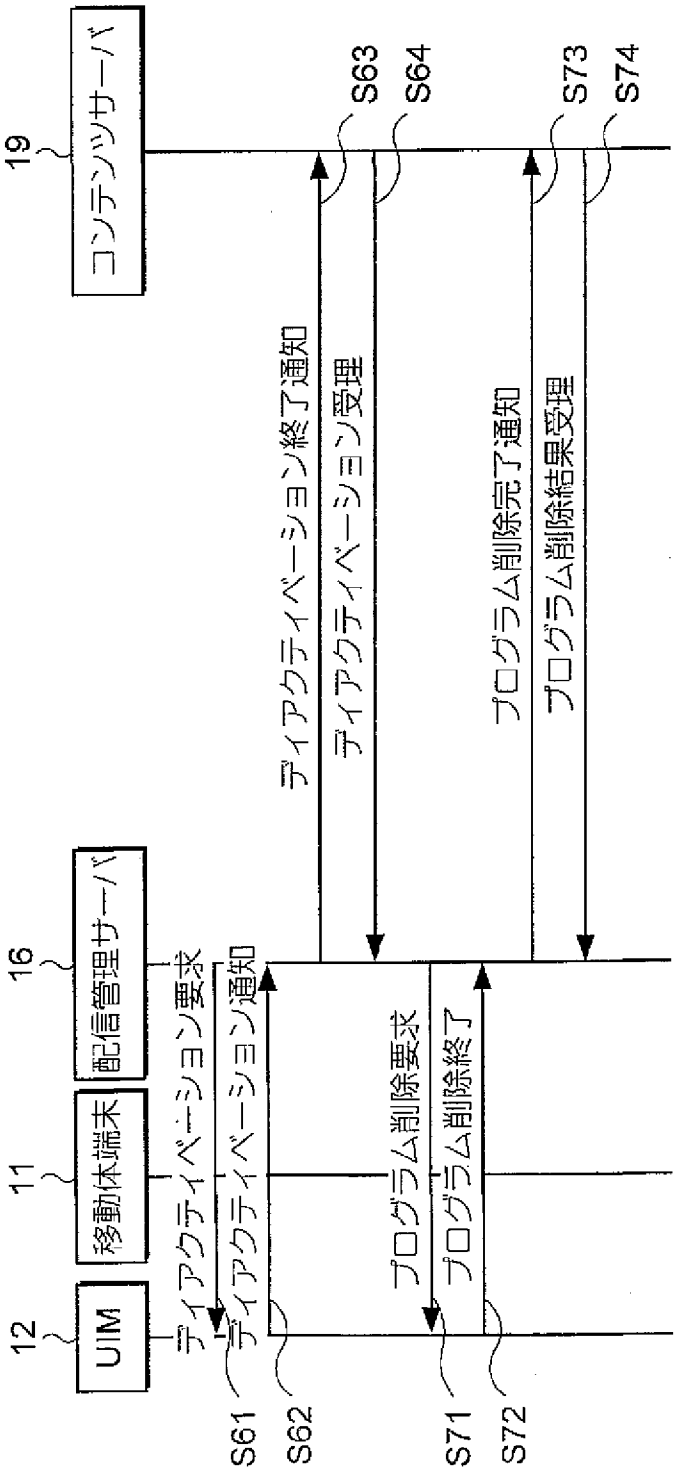

12
UIM
11
移動体端末
16
配信管理サーバ
19
コンテンツサーバ
ディアクティベーション要求
ディアクティベーション通知
ディアクティベーション終了通知
ディアクティベーション受理
プログラム削除要求
プログラム削除終了
プログラム削除完了通知
プログラム削除結果受理
S61
S62
S63
S64
S71
S72
S73
S74

図 12

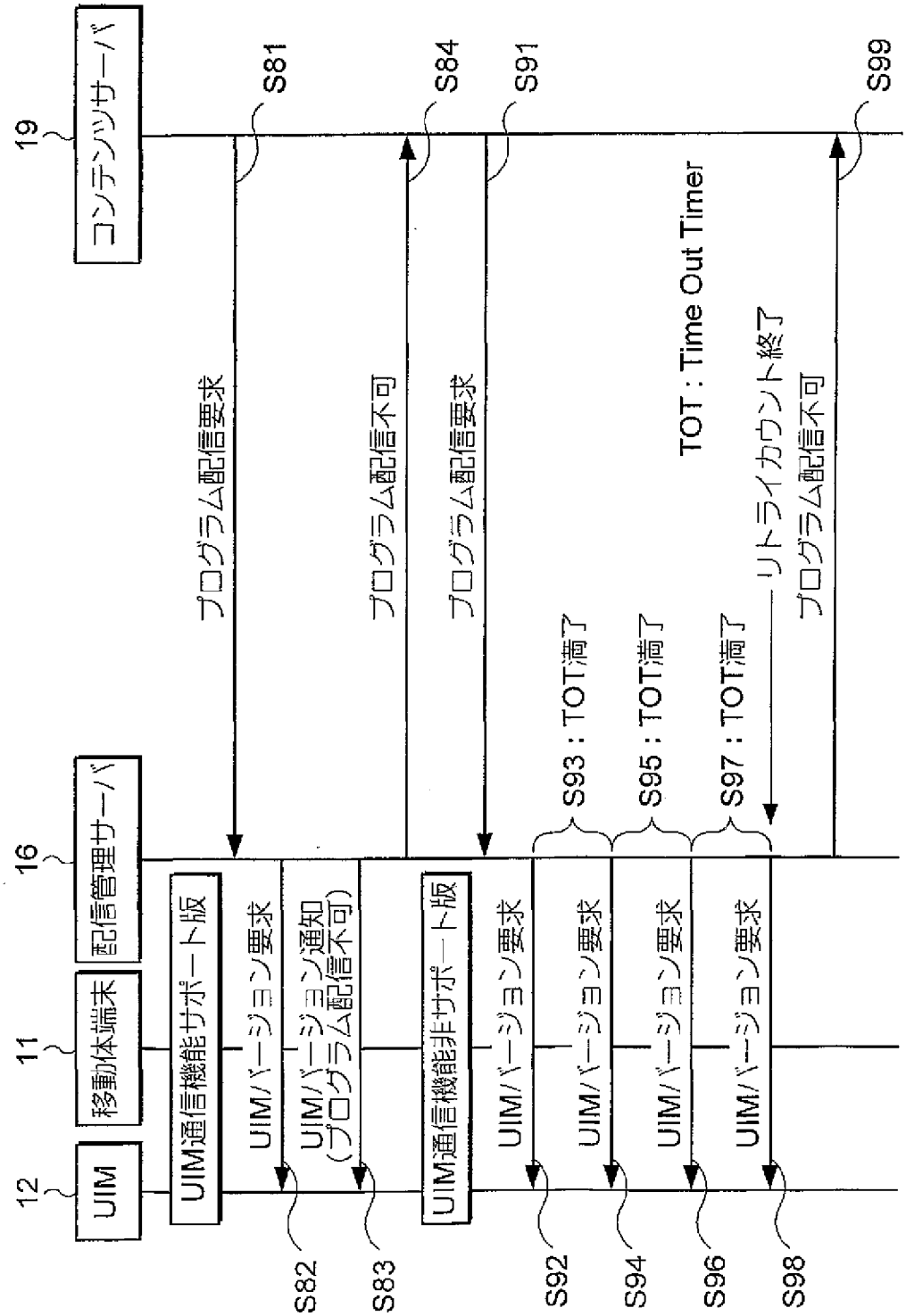

12
UIM
11
移動体端末
16
配信管理サーバ
19
コンテンツサーバ
UIM通信機能サポート版
UIM通信機能非サポート版
UIMバージョン要求
UIMバージョン通知
(プログラム配信不可)
プログラム配信要求
プログラム配信不可
プログラム配信要求
S93：TOT満了
S95：TOT満了
S97：TOT満了
TOT：Time Out Timer
リトライカウント終了
プログラム配信不可
S81
S82
S83
S84
S91
S92
S94
S96
S98
S99

図 13

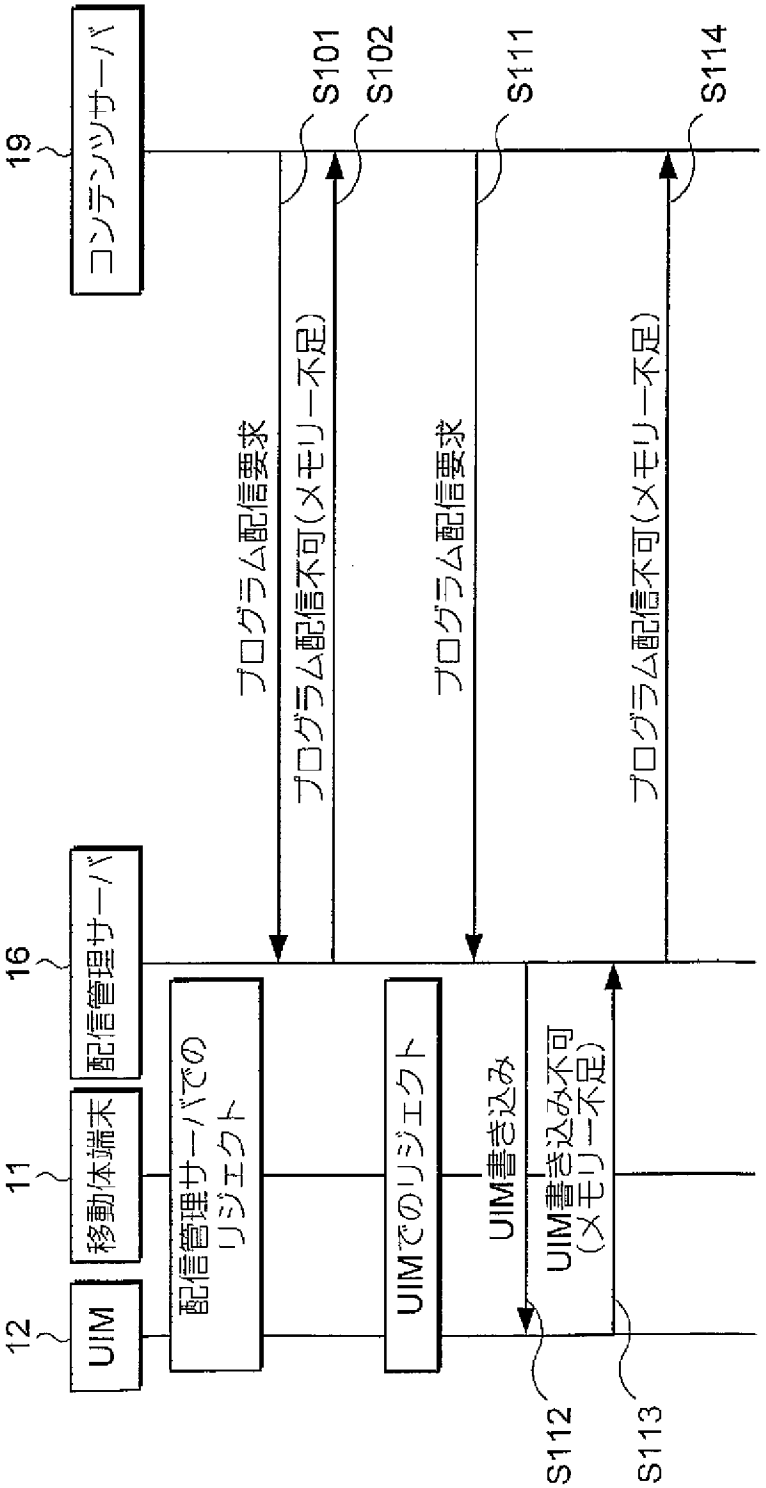

19
コンテンツサーバ
S101
S102
S111
S114
プログラム配信要求
プログラム配信不可(メモリー不足)
プログラム配信要求
プログラム配信不可(メモリー不足)
16
配信管理サーバ
11
移動体端末
12
UIM
配信管理サーバでの
リジェクト
UIMでのリジェクト
UIM書き込み
UIM書き込み不可
(メモリー不足)
S112
S113

図 14

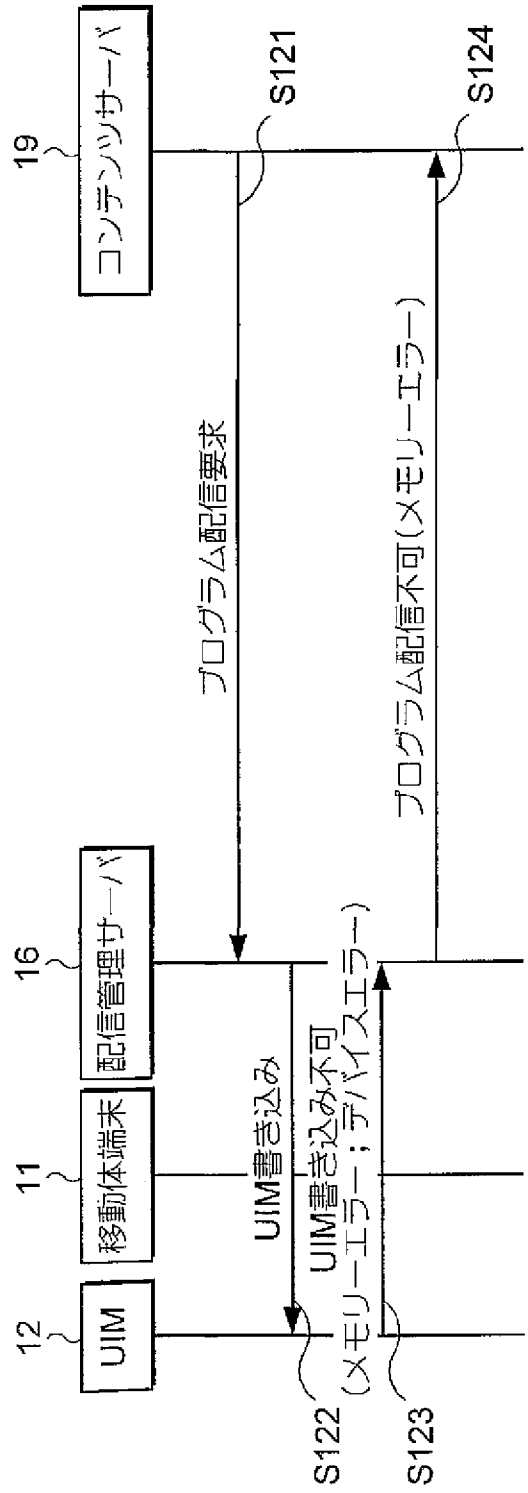

19
コンテンツサーバ
S121
S124
プログラム配信要求
プログラム配信不可（メモリーエラー）
16
配信管理サーバ
11
移動体端末
12
UIM
UIM書き込み
UIM書き込み不可
（メモリーエラー；デバイスエラー）
S122
S123

図 15

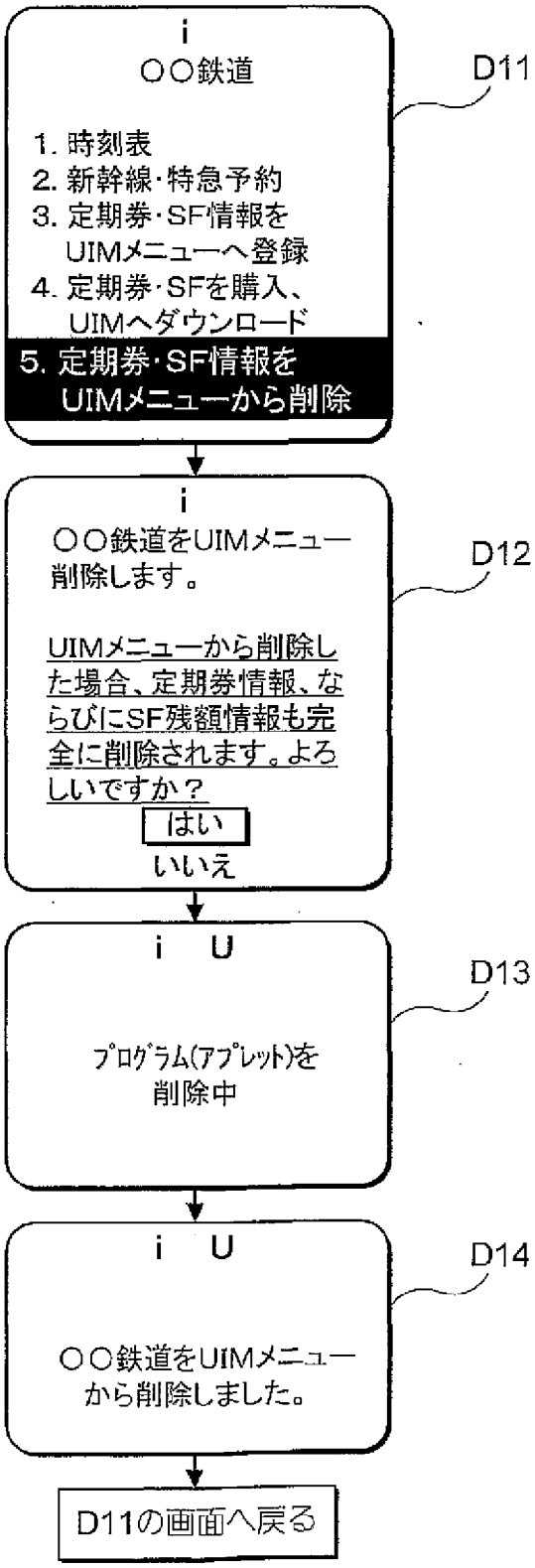

i
○○鉄道
1. 時刻表
2. 新幹線・特急予約
3. 定期券・SF情報を
UIMメニューへ登録
4. 定期券・SFを購入、
UIMへダウンロード
5. 定期券・SF情報を
UIMメニューから削除
D11
i
○○鉄道をUIMメニュー
削除します。
UIMメニューから削除した場合、定期券情報、ならびにSF残額情報も完全に削除されます。よろしいですか？
はい
いいえ
D12
i U
ﾌﾟﾛｸﾞﾗﾑ(ｱﾌﾟﾚｯﾄ)を
削除中
D13
i U
○○鉄道をUIMメニュー
から削除しました。
D14
D11の画面へ戻る

図 16

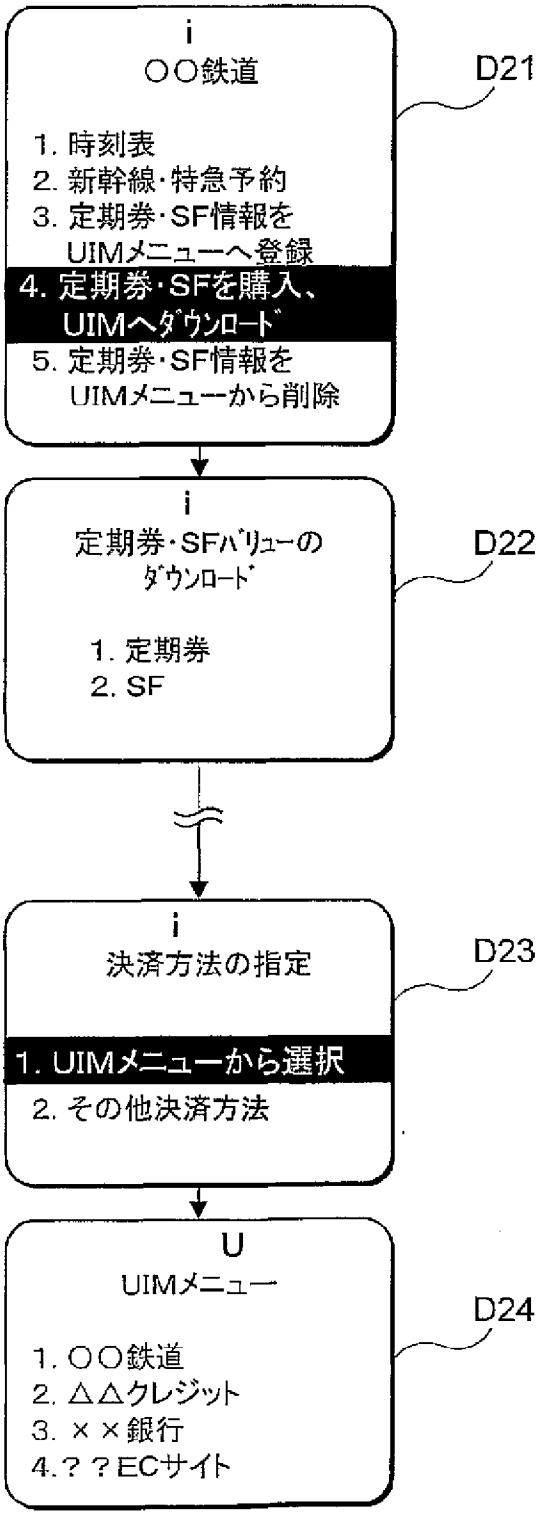

i
○○鉄道
1. 時刻表
2. 新幹線・特急予約
3. 定期券・SF情報を
UIMメニューへ登録
4. 定期券・SFを購入、
UIMへﾀﾞｳﾝﾛｰﾄﾞ
5. 定期券・SF情報を
UIMメニューから削除
D21
i
定期券・SFﾊﾞﾘｭｰの
ﾀﾞｳﾝﾛｰﾄﾞ
1. 定期券
2. SF
D22
i
決済方法の指定
1. UIMメニューから選択
2. その他決済方法
D23
U
UIMメニュー
1. ○○鉄道
2. △△クレジット
3. ××銀行
4.？？ECサイト
D24

図 17

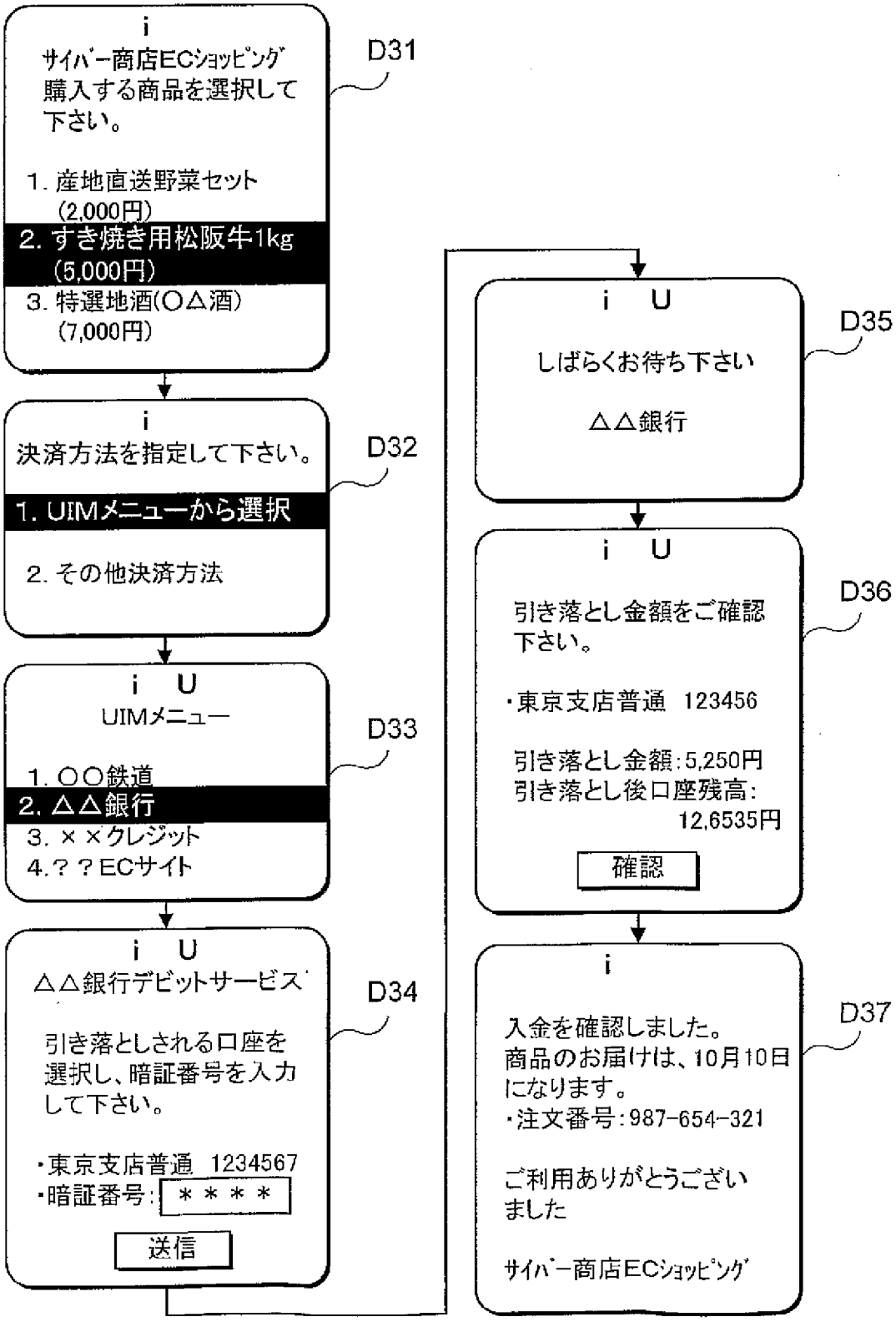

i
ｻｲﾊﾞｰ商店ECｼｮｯﾋﾟﾝｸﾞ
購入する商品を選択して下さい。
1. 産地直送野菜セット (2,000円)
2. すき焼き用松阪牛1kg (5,000円)
3. 特選地酒(○△酒) (7,000円)
D31
i
決済方法を指定して下さい。
1. UIMメニューから選択
2. その他決済方法
D32
i U
UIMメニュー
1. ○○鉄道
2. △△銀行
3. ××クレジット
4. ？？ECサイト
D33
i U
△△銀行デビットサービス
引き落としされる口座を選択し、暗証番号を入力して下さい。
・東京支店普通 1234567
・暗証番号: ＊＊＊＊
送信
D34
i U
しばらくお待ち下さい
△△銀行
D35
i U
引き落とし金額をご確認下さい。
・東京支店普通 123456
引き落とし金額:5,250円
引き落とし後口座残高: 12,6535円
確認
D36
i
入金を確認しました。
商品のお届けは、10月10日になります。
・注文番号:987-654-321
ご利用ありがとうございました
ｻｲﾊﾞｰ商店ECｼｮｯﾋﾟﾝｸﾞ
D37

図 18

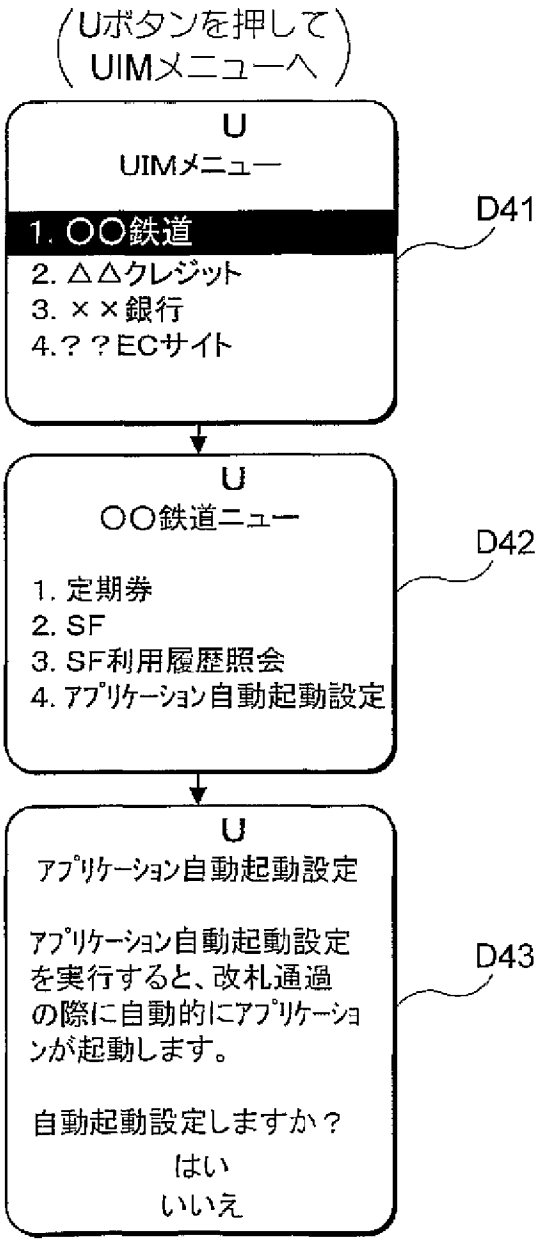

(Uボタンを押して
UIMメニューへ)
U
UIMメニュー
1. ○○鉄道
2. △△クレジット
3. ××銀行
4.？？ECサイト
D41
U
○○鉄道ニュー
1. 定期券
2. SF
3. SF利用履歴照会
4. ｱﾌﾟﾘｹｰｼｮﾝ自動起動設定
D42
U
ｱﾌﾟﾘｹｰｼｮﾝ自動起動設定
ｱﾌﾟﾘｹｰｼｮﾝ自動起動設定
を実行すると、改札通過
の際に自動的にｱﾌﾟﾘｹｰｼｮ
ンが起動します。
自動起動設定しますか？
はい
いいえ
D43

図 19

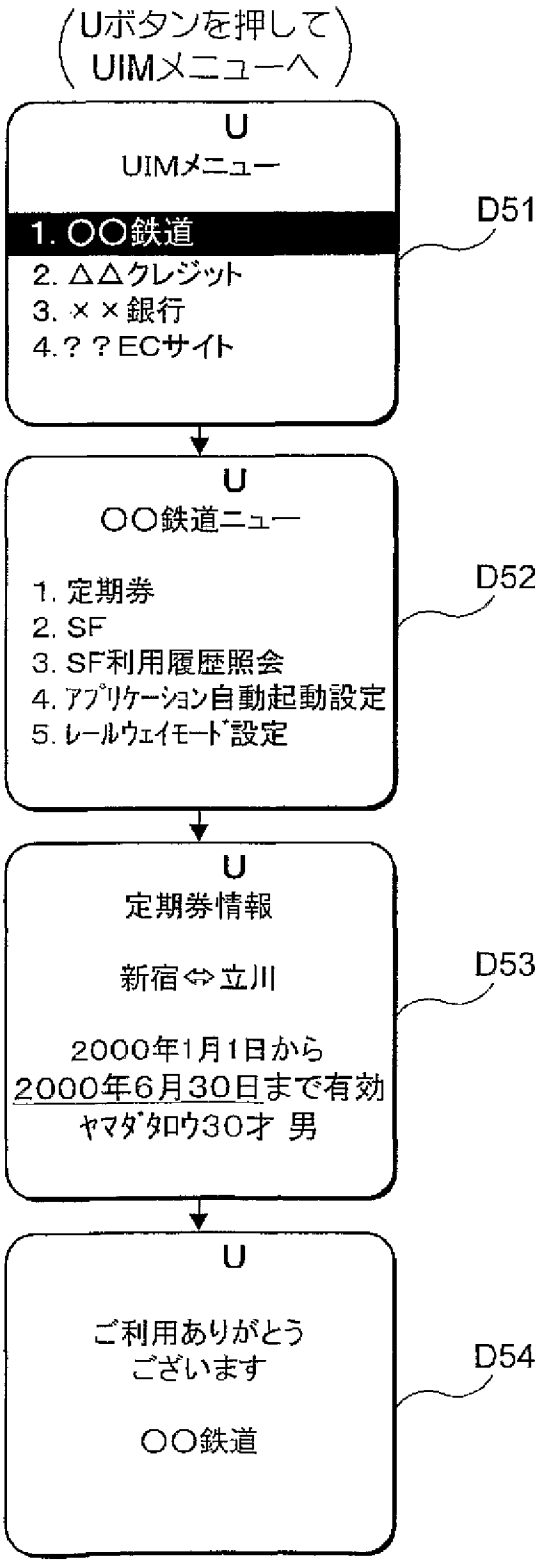

(Uボタンを押して
UIMメニューへ)
U
UIMメニュー
1. ○○鉄道
2. △△クレジット
3. ××銀行
4. ？？ECサイト
D51
U
○○鉄道ニュー
1. 定期券
2. SF
3. SF利用履歴照会
4. ｱﾌﾟﾘｹｰｼｮﾝ自動起動設定
5. ﾚｰﾙｳｪｲﾓｰﾄﾞ設定
D52
U
定期券情報
新宿⇔立川
2000年1月1日から
2000年6月30日まで有効
ﾔﾏﾀﾞﾀﾛｳ30才 男
D53
U
ご利用ありがとう
ございます
○○鉄道
D54

図 20

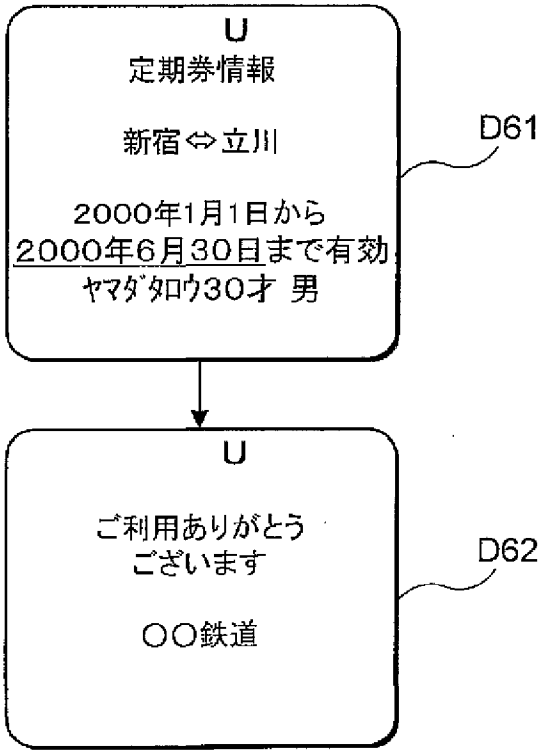

U
定期券情報
新宿⇔立川
2000年1月1日から
2000年6月30日まで有効
ﾔﾏﾀﾞﾀﾛｳ30才 男
D61
U
ご利用ありがとう
ございます
○○鉄道
D62

図 21

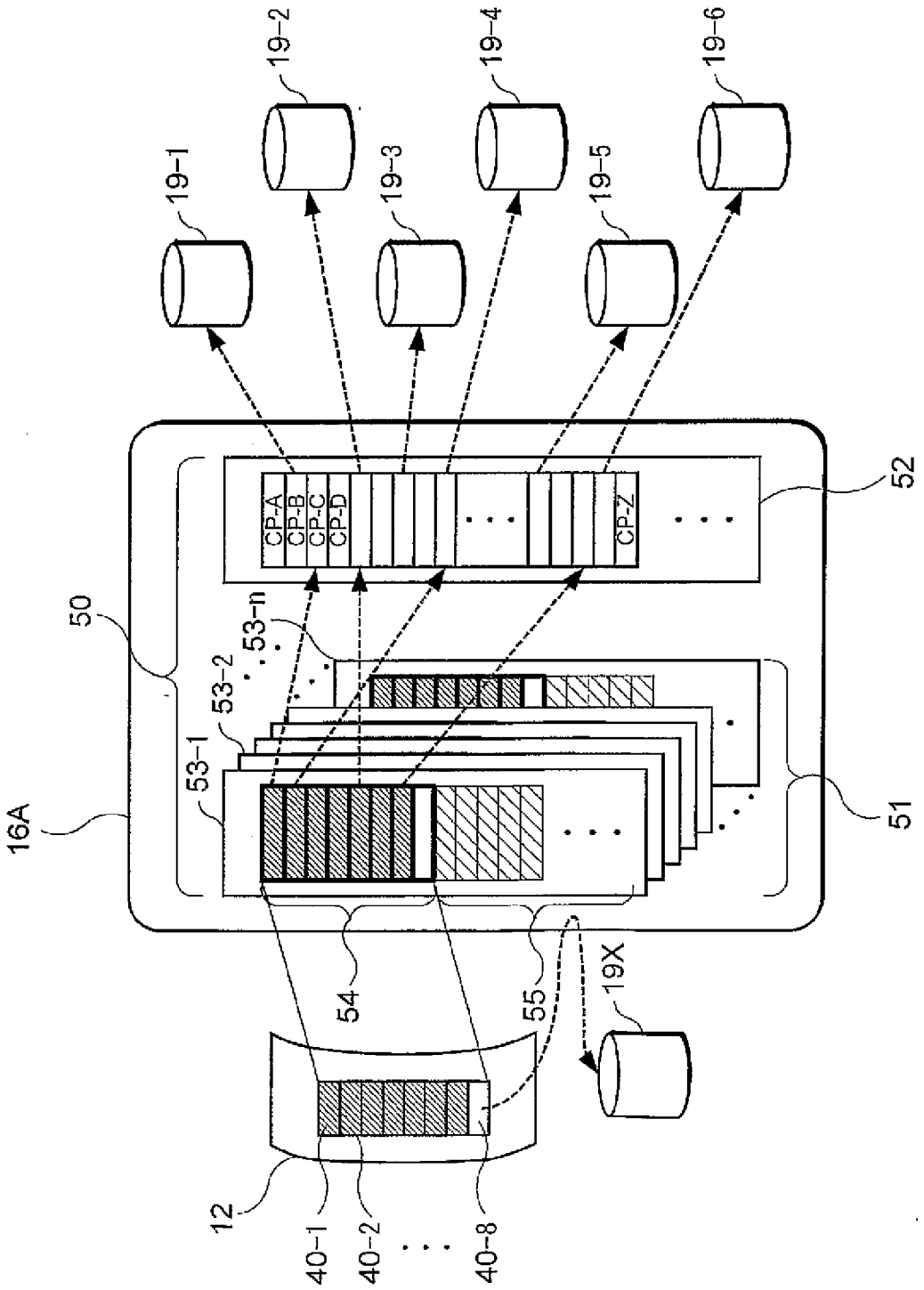

19-1
19-2
19-3
19-4
19-5
19-6
CP-A
CP-B
CP-C
CP-D
CP-Z
52
50
53-n
53-2
53-1
16A
51
54
55
19X
12
40-1
40-2
40-8

図 22

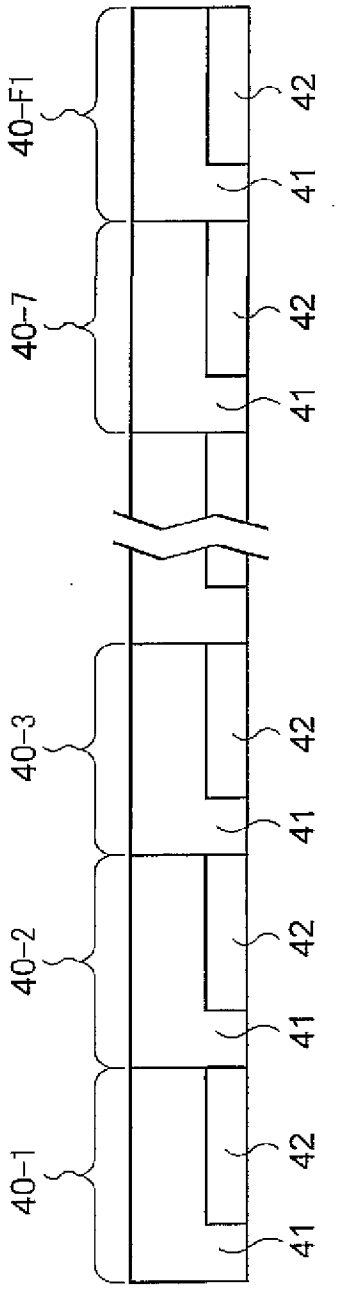


図 23

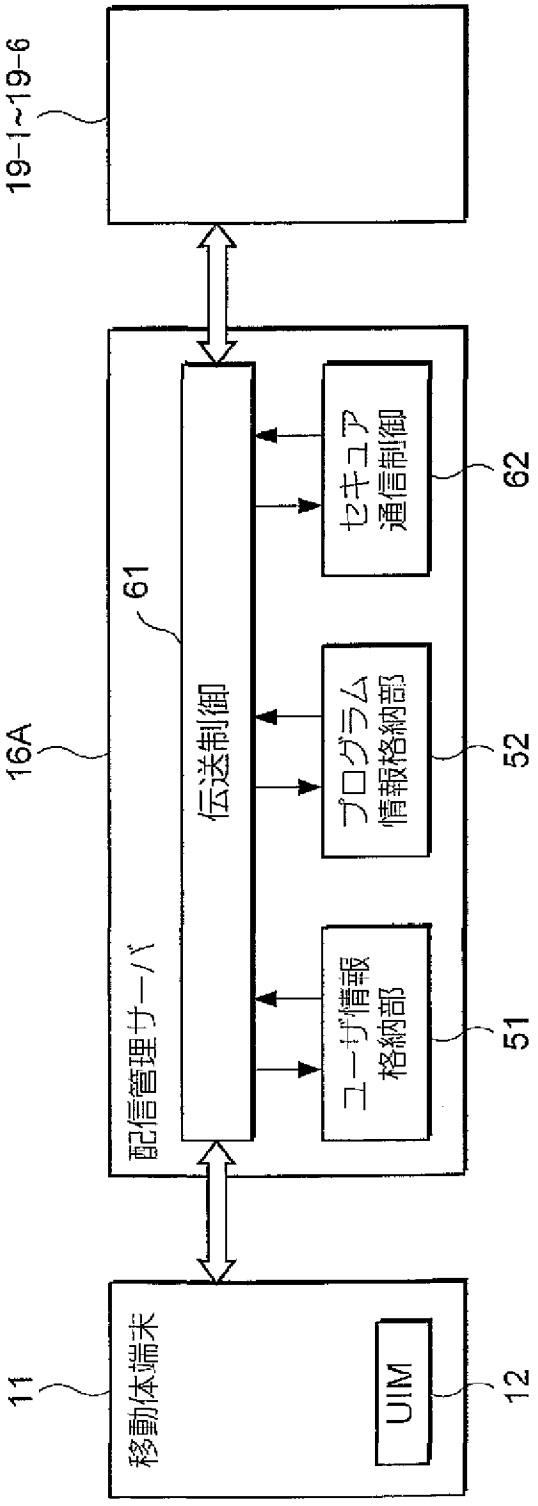

19-1~19-6
16A
61
伝送制御
セキュア
通信制御
62
プログラム
情報格納部
52
ユーザ情報
格納部
51
配信管理サーバ
11
移動体端末
UIM
12

図 24

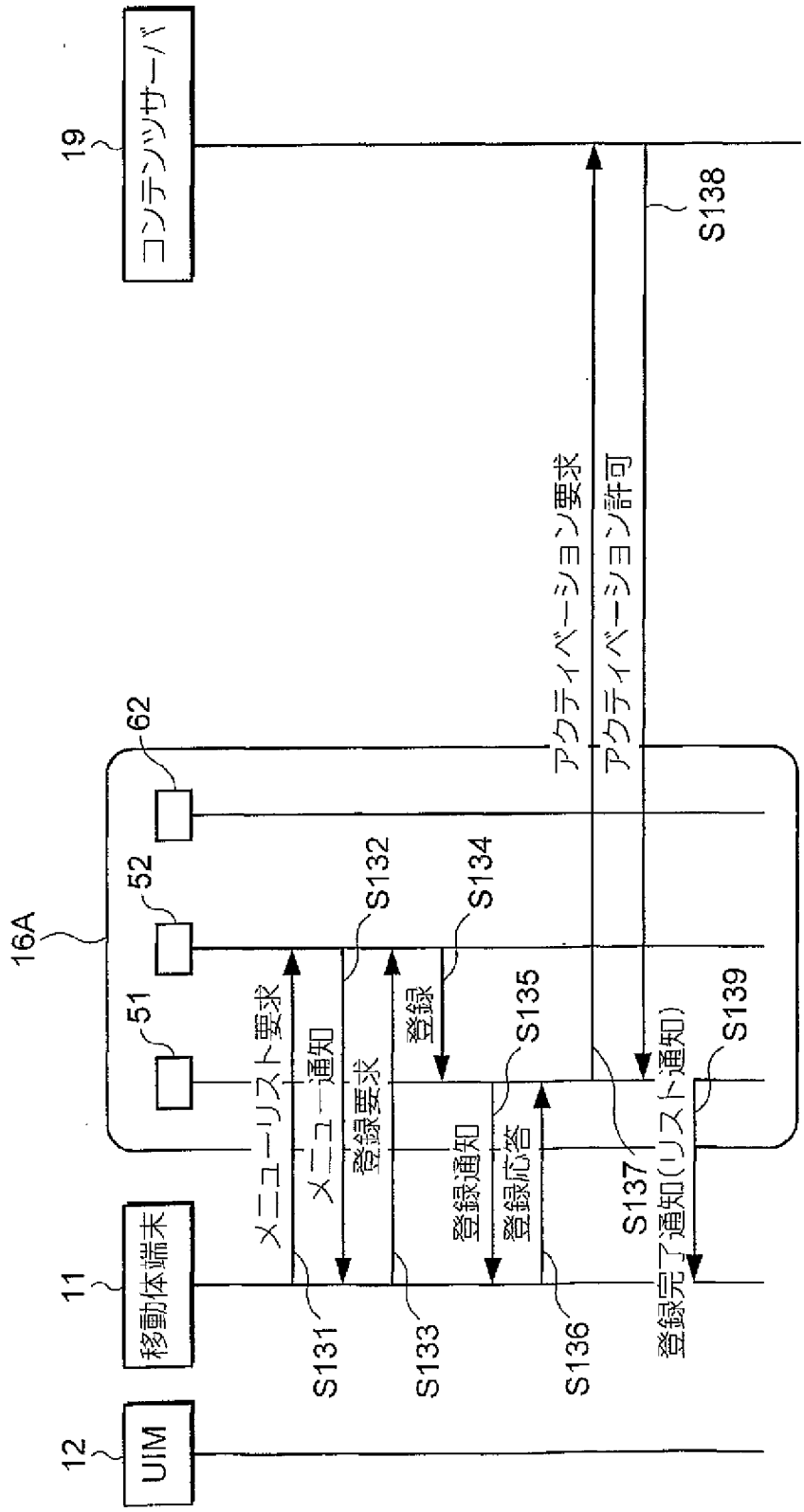

19
コンテンツサーバ
S138
62
52
51
16A
S132
S134
S135
S139
アクティベーション要求
アクティベーション許可
メニューリスト要求
メニュー通知
登録要求
登録
登録通知
登録応答
S137
登録完了通知(リスト通知)
11
移動体端末
12
UIM
S131
S133
S136

図 25

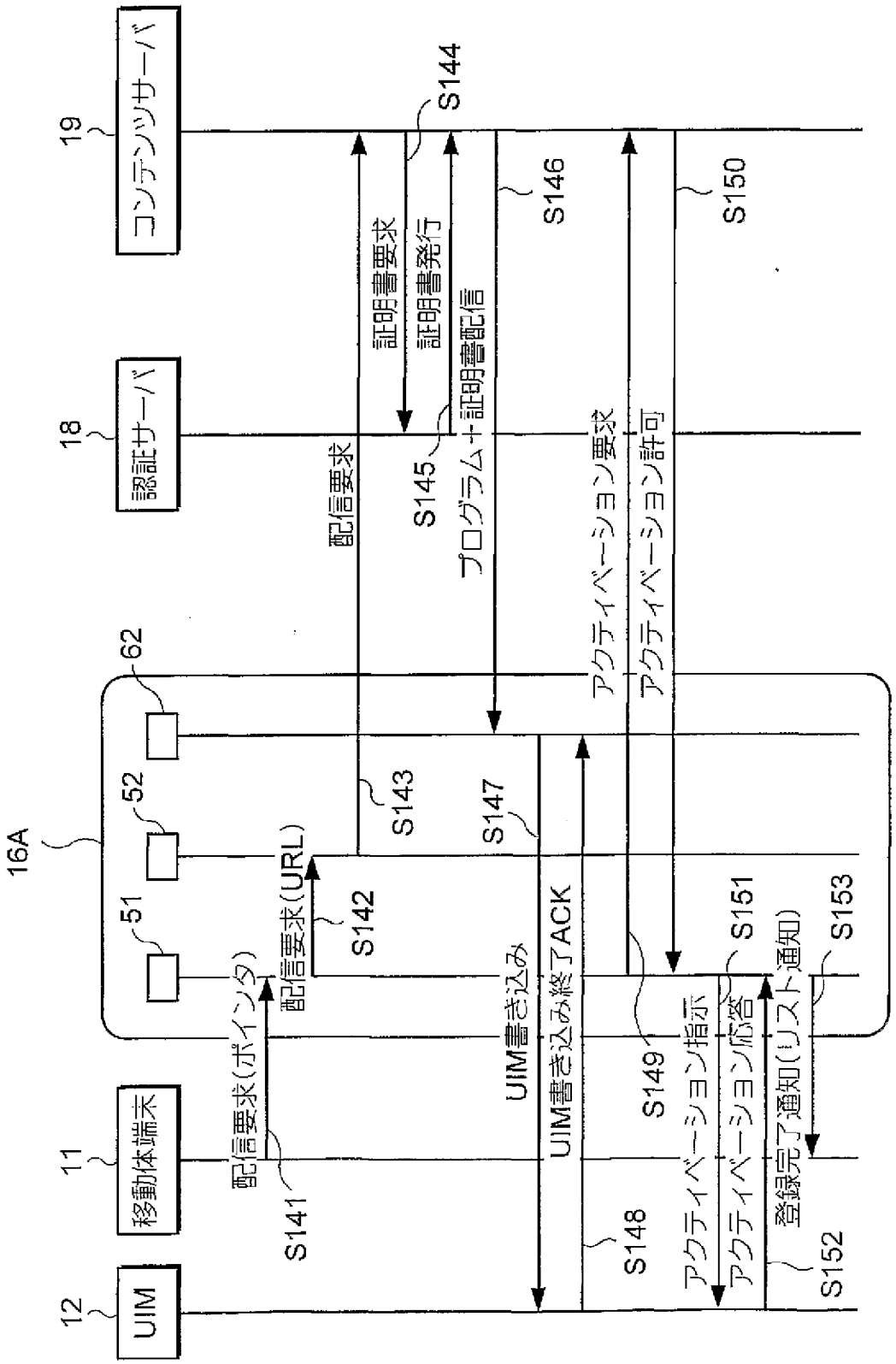

12
UIM
11
移動体端末
16A
51
52
62
18
認証サーバ
19
コンテンツサーバ
S141
配信要求(ポインタ)
S142
配信要求(URL)
S143
配信要求
S144
証明書要求
S145
証明書発行
プログラム＋証明書配信
S146
S147
UIM書き込み
UIM書き込み終了ACK
S148
S149
アクティベーション要求
アクティベーション許可
S150
S151
アクティベーション指示
アクティベーション応答
S152
登録完了通知(リスト通知)
S153

図 26

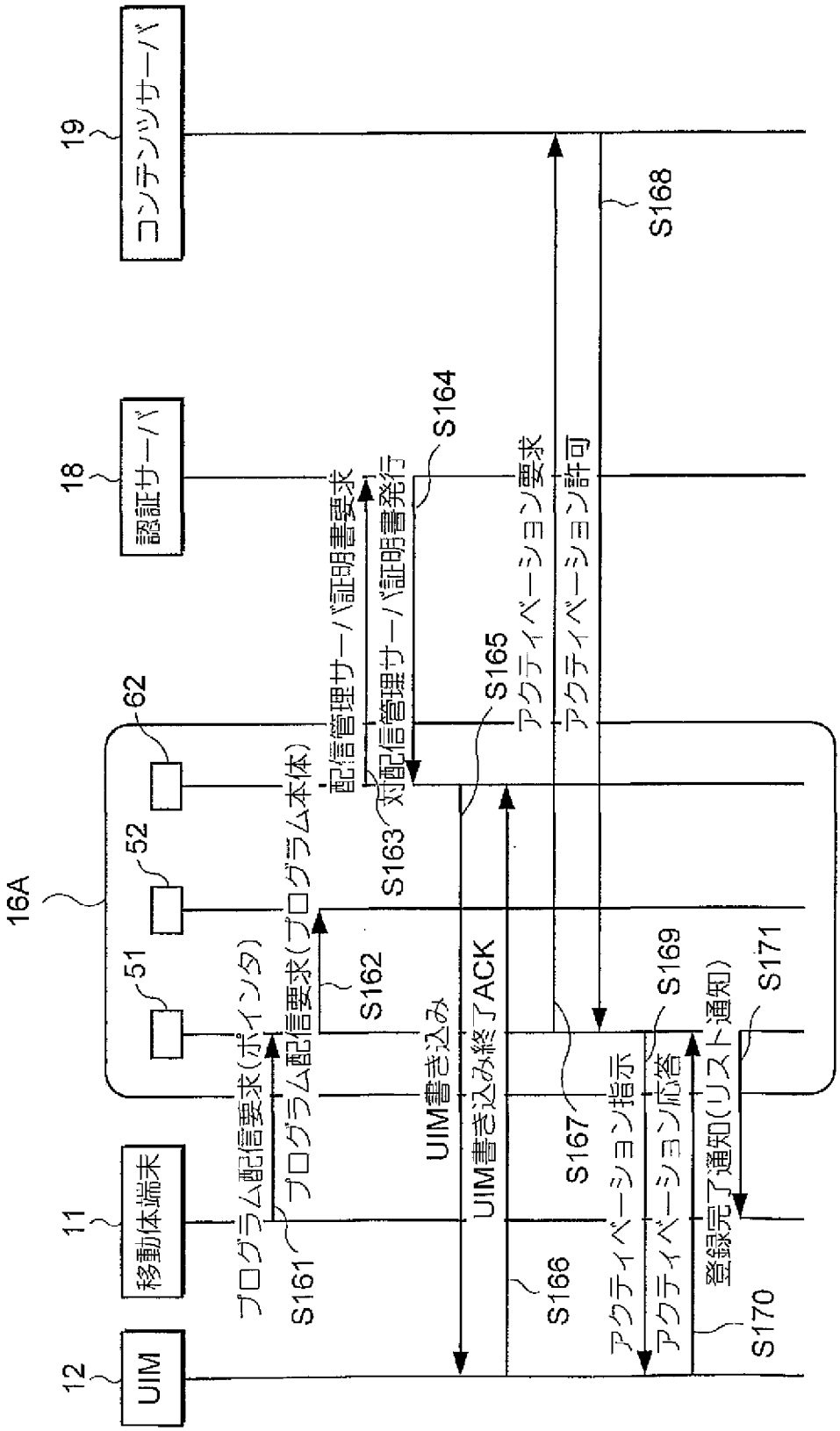

12
UIM
11
移動体端末
16A
51
52
62
18
認証サーバ
19
コンテンツサーバ
プログラム配信要求(ポインタ)
S161
プログラム配信要求(プログラム本体)
S162
配信管理サーバ証明書要求
S163
対配信管理サーバ証明書発行
S164
S165
アクティベーション要求
アクティベーション許可
S168
UIM書き込み
UIM書き込み終了ACK
S166
S167
アクティベーション指示
S169
アクティベーション応答
登録完了通知(リスト通知)
S170
S171

図 27

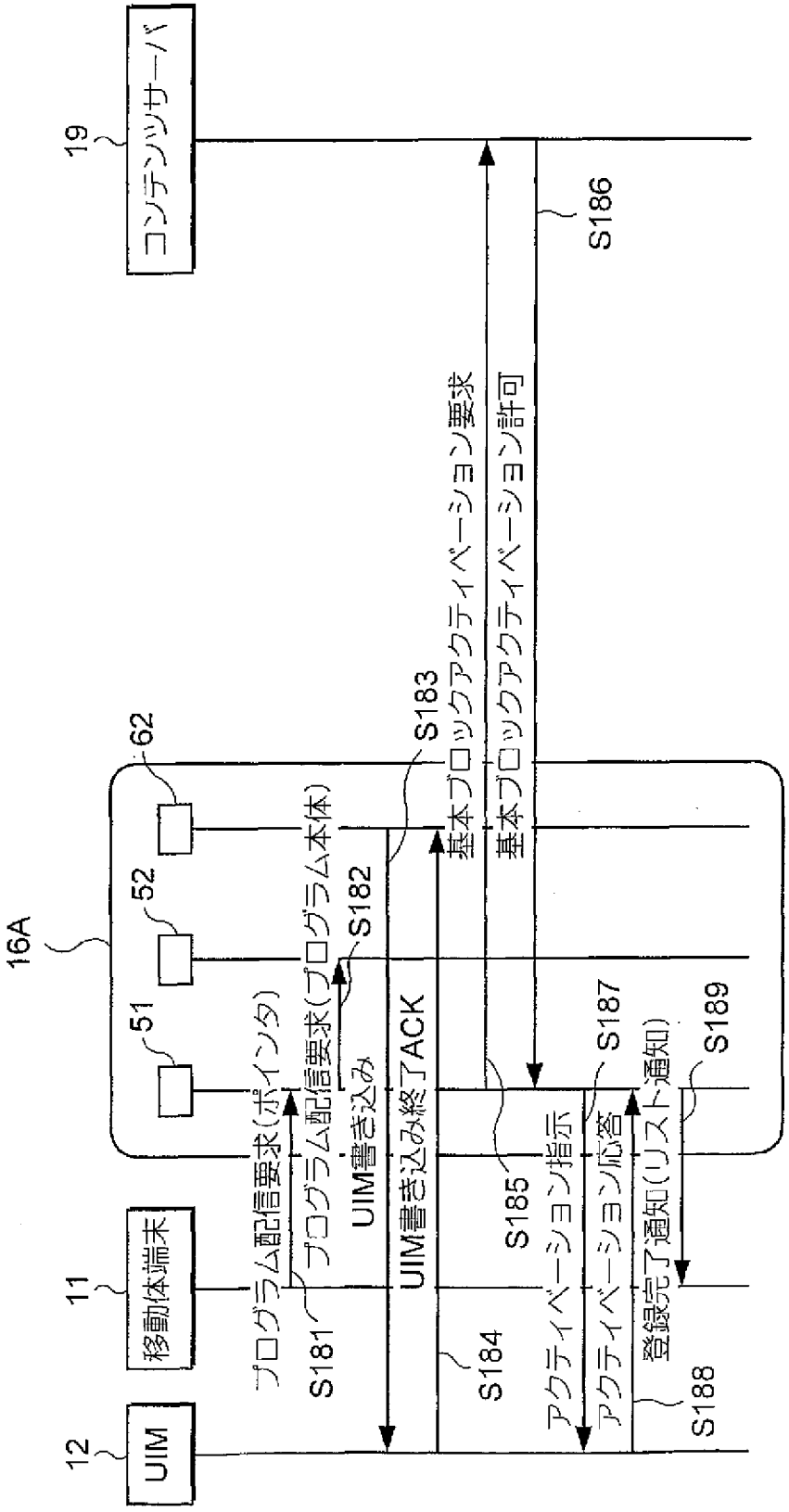

コンテンツサーバ
19
S186
62
S183
基本ブロックアクティベーション要求
基本ブロックアクティベーション許可
16A
52
S182
51
プログラム配信要求(プログラム本体)
UIM書き込み
UIM書き込み終了ACK
S187
S189
プログラム配信要求(ポインタ)
移動体端末
11
S181
S185
アクティベーション指示
アクティベーション応答
登録完了通知(リスト通知)
S184
S188
UIM
12

図 28

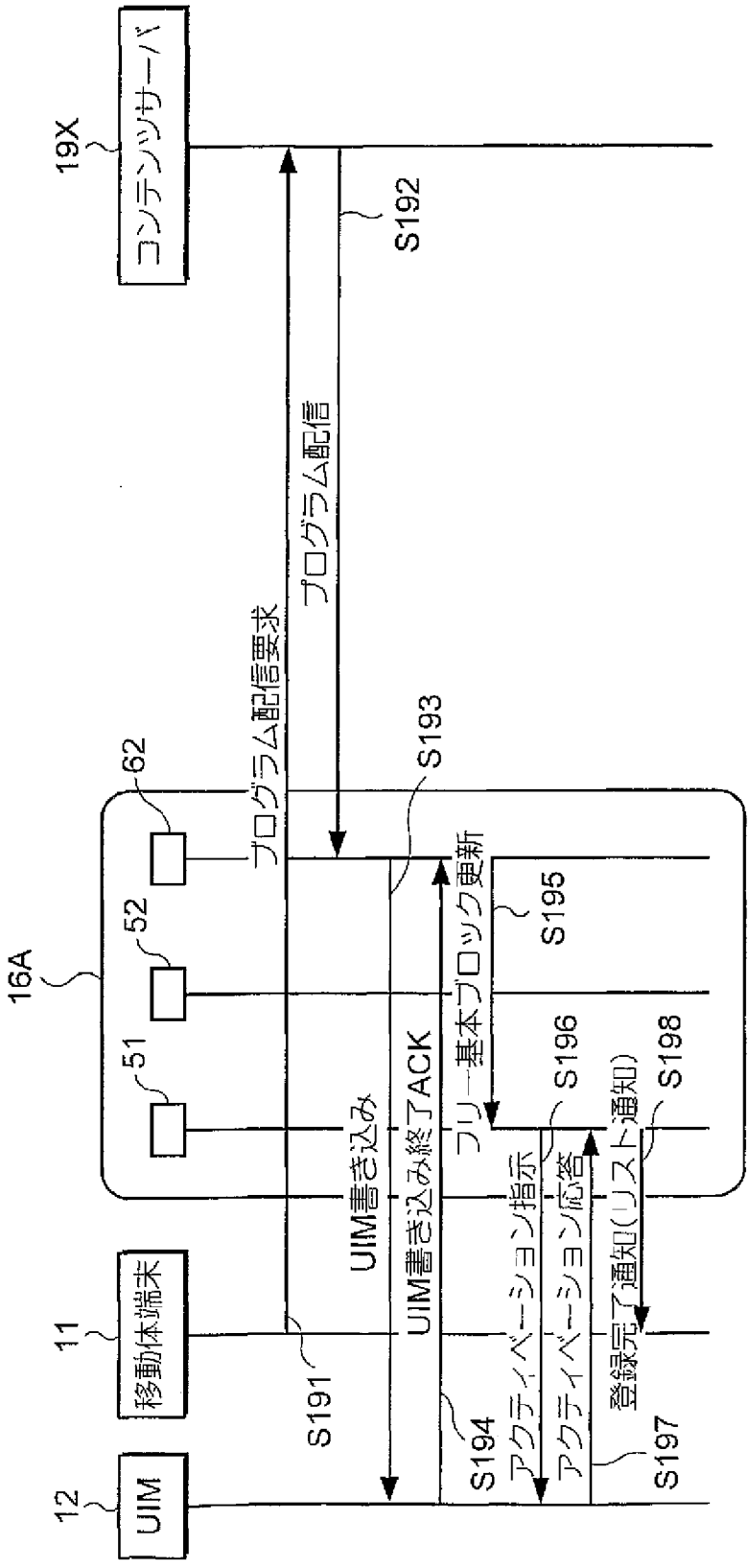

19X
コンテンツサーバ
S192
プログラム配信
プログラム配信要求
S193
62
52
51
16A
フリー基本ブロック更新
S195
S196
S198
UIM書き込み
UIM書き込み終了ACK
アクティベーション指示
アクティベーション応答
登録完了通知(リスト通知)
S191
S194
S197
11
移動体端末
12
UIM

図 29

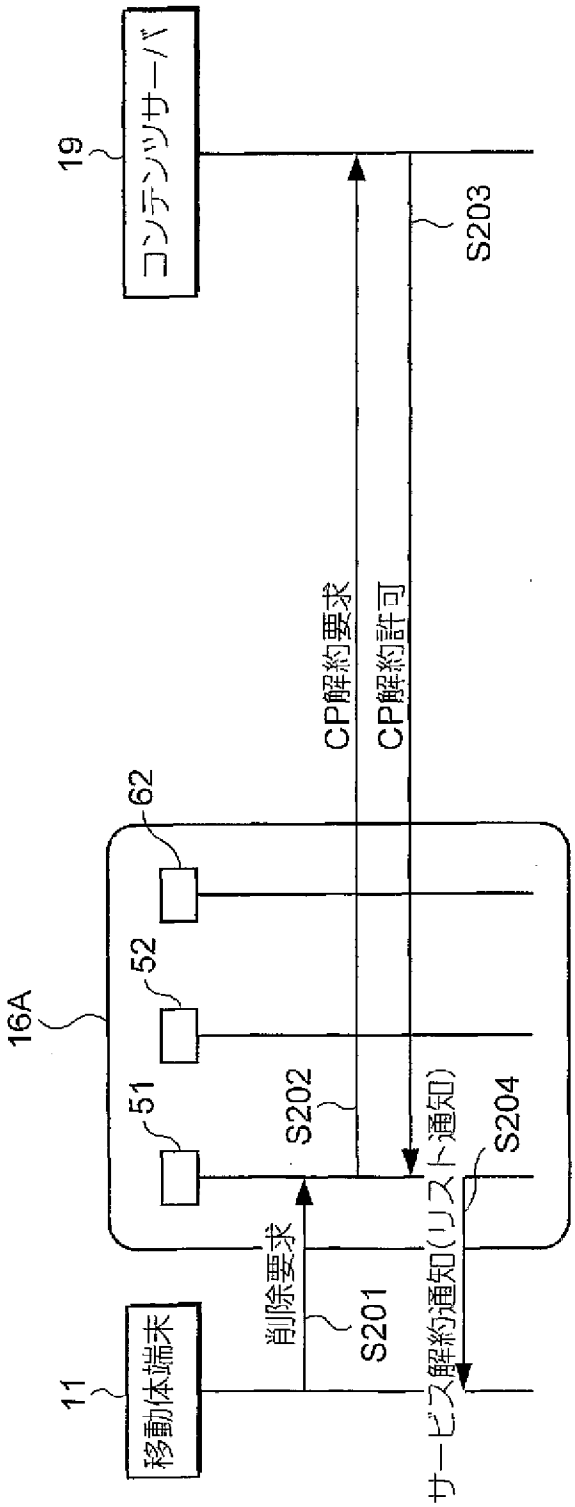

19
コンテンツサーバ
S203
CP解約要求
CP解約許可
62
52
16A
51
S202
S204
削除要求
S201
11
移動体端末
サービス解約通知(リスト通知)

図 30

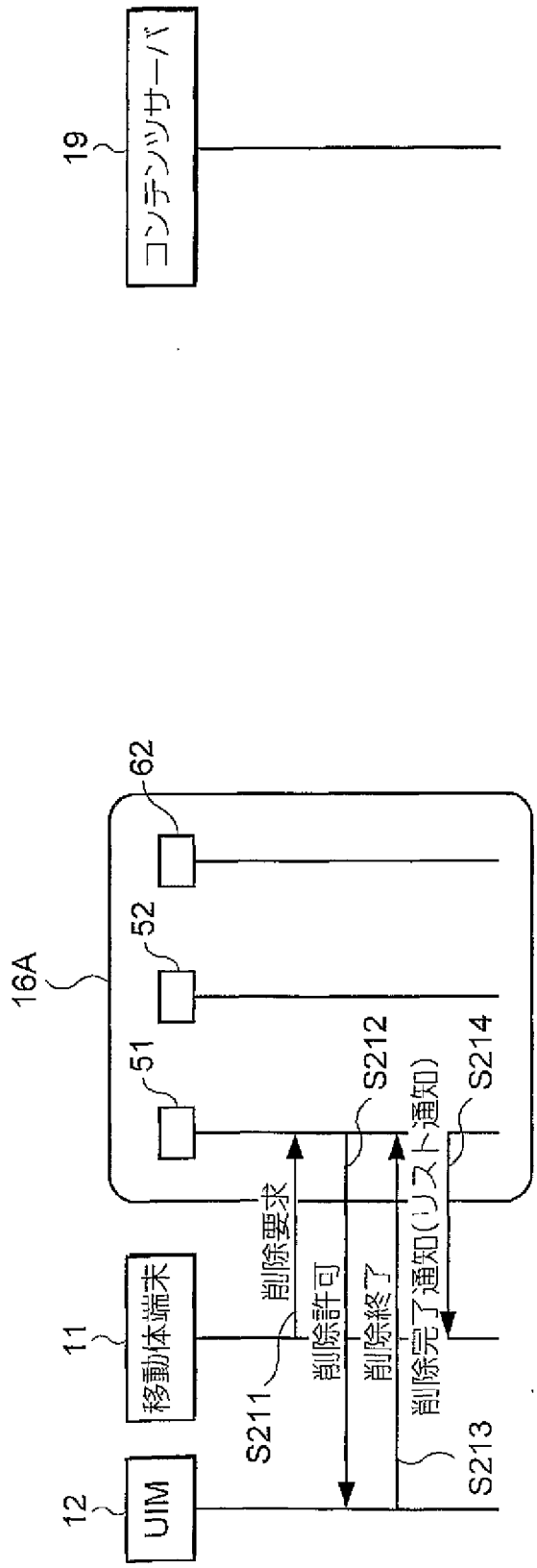

19
コンテンツサーバ
62
52
16A
51
S212
S214
削除要求
削除許可
削除終了
削除完了通知(リスト通知)
11
移動体端末
S211
S213
12
UIM

図 31

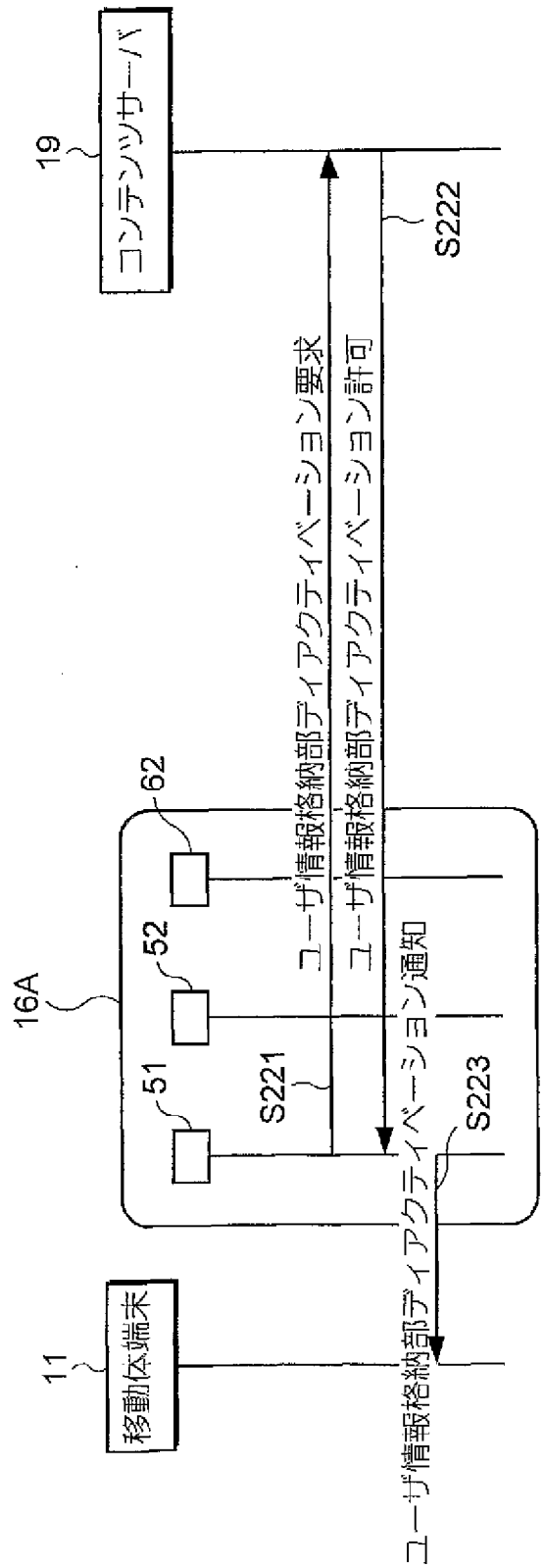
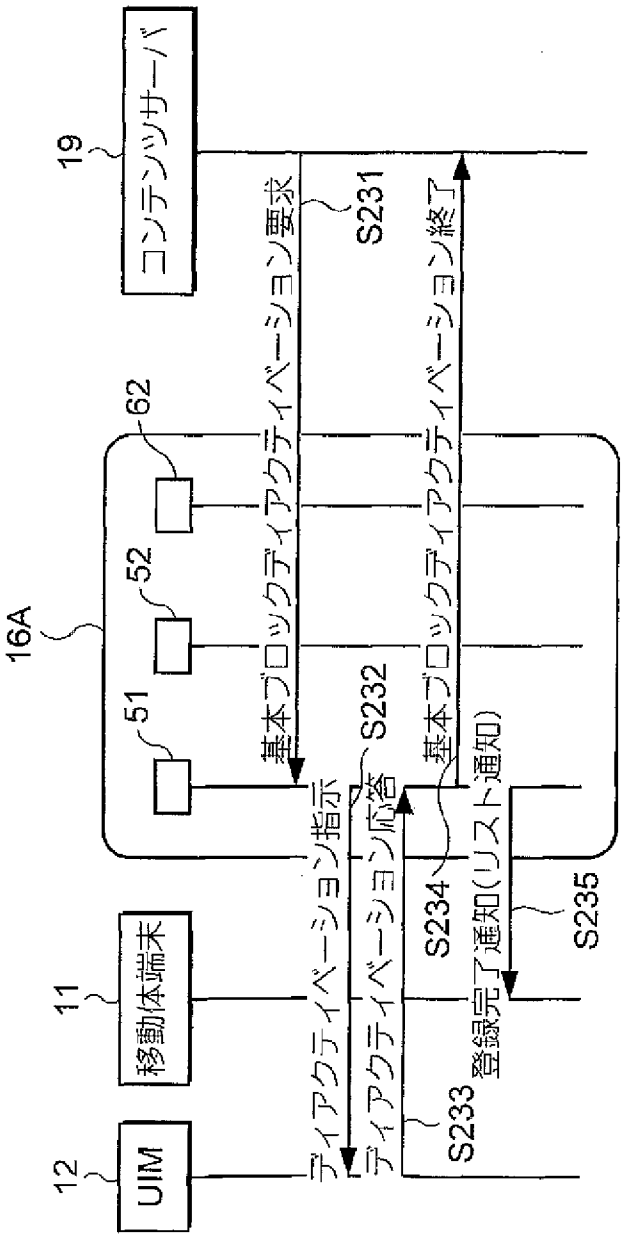

19
コンテンツサーバ
S222
ユーザ情報格納部ディアクティベーション要求
ユーザ情報格納部ディアクティベーション許可
62
52
16A
51
S221
S223
ユーザ情報格納部ディアクティベーション通知
11
移動体端末

図 32


19
コンテンツサーバ
S231
62
52
16A
51
基本ブロックディアクティベーション要求
S232
基本ブロックディアクティベーション終了
ディアクティベーション指示
ディアクティベーション応答
S234
登録完了通知(リスト通知)
S235
S233
11
移動体端末
12
UIM

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/00699

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F9/06, G06F9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F9/06, G06F9/445

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Toroku Jitsuyo Shinan Koho	1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2001-28786 A (Sanyo Electric Co., Ltd.), 30 January, 2001 (30.01.01), Full text; Figs. 1 to 13 (Family: none)	1,3-20,22, 24-26,28,29, 31,36,37,39 2,21,23,27, 30,32-35,38
Y	JP 2000-293584 A (Chugoku Nihon Denki Software Kabushiki Kaisha), 20 October, 2000 (20.10.00), Full text; Figs. 1 to 6 (Family: none)	1,3-20,22, 24-26,28,29, 31,36,37,39
Y	JP 10-78867 A (Hitachi, Ltd.), 24 March, 1998 (24.03.98), Full text; Figs. 1 to 19 (Family: none)	4-7,11,12

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 08 May, 2002 (08.05.02)	Date of mailing of the international search report 21 May, 2002 (21.05.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/00699

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 6-195217 A (Nippon Telegraph And Telephone Corp.), 15 July, 1994 (15.07.94), Full text; Fig. 1 (Family: none)	8,9,25

国際調査報告

国際出願番号　PCT／JP02／00699

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F9／06, G06F9／445

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F9／06, G06F9／445

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926年－1996年
日本国公開実用新案公報　1971年－2002年
日本国実用新案登録公報　1996年－2002年
日本国登録実用新案公報　1994年－2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　2001－28786　A（三洋電機株式会社）2001．01．30，全文，第1－13図（ファミリーなし）	1, 3-20, 22, 24-26, 28, 29, 31, 36, 37, 39
A		2, 21, 23, 27, 30, 32-35, 38
Y	JP　2000－293584　A（中国日本電気ソフトウェア株式会社）2000．10．20，全文，第1－6図（ファミリーなし）	1, 3-20, 22, 24-26, 28, 29, 31, 36, 37, 39

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
08．05．02	21.05.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	漆原　孝治	5B　9366
	電話番号　03－3581－1101　内線　3546	

様式PCT／ISA／210（第2ページ）（1998年7月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　１０－７８８６７　Ａ（株式会社日立製作所） １９９８．０３．２４，全文，第１－１９図（ファミリーなし）	4-7, 11, 12
Ｙ	ＪＰ　６－１９５２１７　Ａ（日本電信電話株式会社） １９９４．０７．１５，全文，第１図（ファミリーなし）	8, 9, 25

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 October 2002 (10.10.2002)

PCT

(10) International Publication Number
WO 02/080449 A1

(51) International Patent Classification[7]: H04L 9/08, H04Q 7/38

(21) International Application Number: PCT/US02/09835

(22) International Filing Date: 28 March 2002 (28.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/279,970 28 March 2001 (28.03.2001) US
09/933,972 20 August 2001 (20.08.2001) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morhouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventors: HAWKES, Philip; 2/6-8 Belmore Street, Burwood, NSW 2134 (AU). ROSE, Gregory, G.; 6 Kingston Avenue, Mortlake, NSW 2137 (AU). HSU, Raymond, T.; 17775 Pennacook Court, San Diego, CA 92127 (US). REZAIIFAR, Ramin; 10896 Caminito Arcada, San Diego, CA 92131 (US).

(74) Agents: WADSWORTH, Philip, R. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

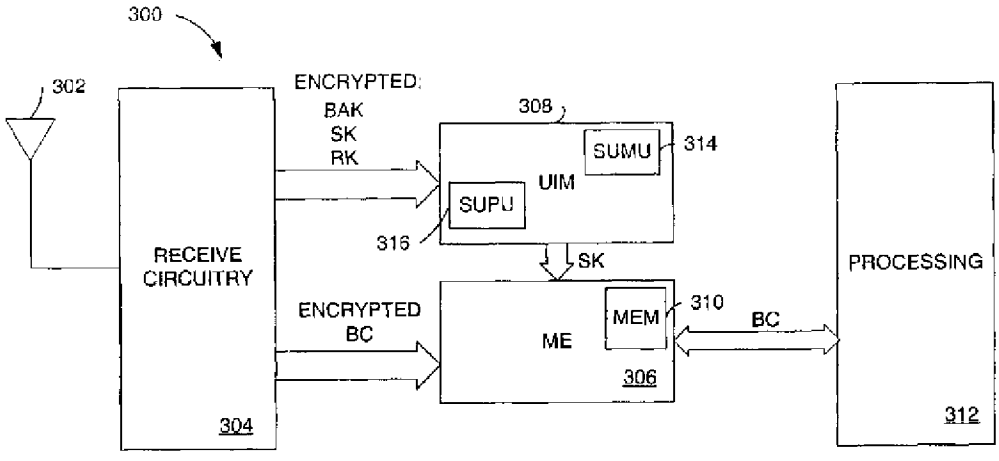
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM



(57) Abstract: Method and apparatus for secure transmissions. Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user. A short-time updated key is encrypted using the broadcast key and provided periodically to a user. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.

WO 02/080449 A1

METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM

BACKGROUND

Claim of Priority under 35 U.S.C. §120

[1001] The present Application for Patent claims priority of U.S. Provisional Application No. 60/279,970, filed March 28,2001, assigned to the assignee hereof and hereby expressly incorporated by reference herein.

Reference to Co-Pending Applications for Patent

[1002] The present invention is related to the following Applications for Patent in the U.S. Patent & Trademark Office:

"METHOD AND APPARATUS FOR OVERHEAD MESSAGING IN A WIRELESS COMMUNICATION SYSTEM" by Nikolai Leung, having Attorney Docket No. 010439, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR OUT-OF-BAND TRANSMISSION OF BROADCAST SERVICE OPTION IN A WIRELESS COMMUNICATION SYSTEM" by Nikolai Leung, having Attorney Docket No. 010437, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR BROADCAST SIGNALING IN A WIRELESS COMMUNICATION SYSTEM" by Nikolai Leung, having Attorney Docket No. 010438, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR TRANSMISSION FRAMING IN A WIRELESS COMMUNICATION SYSTEM" by Raymond Hsu, having Attorney Docket No. 010498, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein;

"METHOD AND APPARATUS FOR DATA TRANSPORT IN A WIRELESS COMMUNICATION SYSTEM" by Raymond Hsu, having Attorney Docket No. 010499, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein; and

"METHOD AND APPARATUS FOR HEADER COMPRESSION IN A WIRELESS COMMUNICATION SYSTEM" by Raymond Hsu, having Attorney Docket No. 010500, filed concurrently herewith and assigned to the assignee hereof, and which is expressly incorporated by reference herein.

Field

[1003] The present invention relates to data processing systems generally and specifically, to methods and apparatus for security in a data processing system.

Background

[1004] Security in data processing and information systems, including communications systems, contributes to accountability, fairness, accuracy, confidentiality, operability, as well as a plethora of other desired criteria. Encryption, or the general field of cryptography, is used in electronic commerce, wireless communications, broadcasting, and has an unlimited range of applications. In electronic commerce, encryption is used to prevent fraud in and verify financial transactions. In data processing systems, encryption is used to verify a participant's identity. Encryption is also used to prevent hacking, protect Web pages, and prevent access to confidential documents.

[1005] Asymmetric encryption system, often referred to as a cryptosystem, uses a same key (i.e., the secret key) to encrypt and decrypt a message. Whereas an asymmetric encryption system uses a first key (i.e., the public key) to encrypt a message and uses a different key (i.e., the private key) to decrypt it. Asymmetric cryptosystems are also called public key cryptosystems. A problem exists in symmetric cryptosystems in the secure provision of the secret key from a sender to a recipient. Further, a problem exists when keys or other encryption mechanisms are updated frequently. In a data processing system

methods of securely updating keys incur processing time, memory storage and other processing overhead. In a wireless communication system, updating keys uses valuable bandwidth used for transmission.

[1006] The prior art does not provide a method for updating keys to a large group of mobile stations in order that they may access an encrypted broadcast. There is a need, therefore, for a secure and efficient method of updating keys in a data processing system. Further, there is a need for a secure and efficient method of updating keys in a wireless communication system.

SUMMARY

[1007] Embodiments disclosed herein address the above stated needs by providing a method for security in a data processing system.

[1008] In one aspect a method for secure transmissions includes determining a registration key specific to a participant in a transmission, determining a first key, encrypting the first key with the registration key, determining a second key, encrypting the second key with the first key and updating the first and second keys.

[1009] In another aspect, a method for secure reception of a transmission includes receiving a registration key specific to a participant in a transmission, receiving a first key, decrypting the first key with the registration key, receiving a second key, decrypting the second key with the first key, receiving a broadcast stream of information, and decrypting the broadcast stream of information using the second key.

[1010] In still another aspect a wireless communication system supporting a broadcast service option has an infrastructure element including a receive circuitry, a user identification unit, operative to recover a short-time key for decrypting a broadcast message, and a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message. The user identification unit includes a processing unit operative to decrypt key information, and a memory storage unit for storing a registration key.

BRIEF DESCRIPTION OF THE DRAWINGS

[1011] FIG. 1A is a diagram of a cryptosystem.

[1012] FIG. 1B is a diagram of a symmetric cryptosystem.

[1013] FIG. 1C is a diagram of an asymmetric cryptosystem.

[1014] FIG. 1D is a diagram of a PGP encryption system.

[1015] FIG. 1E is a diagram of a PGP decryption system.

[1016] FIG. 2 is a diagram of a spread spectrum communication system that supports a number of users.

[1017] FIG. 3 is a block diagram of the communication system supporting broadcast transmissions.

[1018] FIG. 4 is a block diagram of a mobile station in a wireless communication system.

[1019] FIG. 5 is a model describing the updating of keys within a mobile station used for controlling broadcast access.

[1020] FIG. 6 is a model describing cryptographic operations within a UIM.

[1021] FIGs. 7A-7D illustrate a method of implementing security encryption in a wireless communication system supporting broadcast transmissions.

[1022] FIG. 7E is a timing diagram of key update periods of a security option in a wireless communication system supporting broadcast transmissions.

[1023] FIGs. 8A-8D illustrate application of a security encryption method in a wireless communication system supporting broadcast transmissions.

DETAILED DESCRIPTION

[1024] The word "exemplary" is used exclusively herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[1025] Wireless communication systems are widely deployed to provide various types of communication such as voice, data, and so on. These systems may be based on code division multiple access (CDMA), time division multiple access (TDMA), or some other modulation techniques. A CDMA system

provides certain advantages over other types of system, including increased system capacity.

[1026] A system may be designed to support one or more standards such as the "TIA/EIA/IS-95-B Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System" referred to herein as the IS-95 standard, the standard offered by a consortium named "3rd Generation Partnership Project" referred to herein as 3GPP, and embodied in a set of documents including Document Nos. 3G TS 25.211, 3G TS 25.212, 3G TS 25.213, and 3G TS 25.214, 3G TS 25.302, referred to herein as the W-CDMA standard, the standard offered by a consortium named "3rd Generation Partnership Project 2" referred to herein as 3GPP2, and TR-45.5 referred to herein as the cdma2000 standard, formerly called IS-2000 MC. The standards cited hereinabove are hereby expressly incorporated herein by reference.

[1027] Each standard specifically defines the processing of data for transmission from base station to mobile, and vice versa. As an exemplary embodiment the following discussion considers a spread-spectrum communication system consistent with cdma2000 systems. Alternate embodiments may incorporate another standard/system. Still other embodiments may apply the security methods disclosed herein to any type of data processing system using a cryptosystem.

[1028] A cryptosystem is a method of disguising messages thus allowing a specific group of users to extract the message. FIG. 1A illustrates a basic cryptosystem 10. Cryptography is the art of creating and using cryptosystems. Cryptanalysis is the art of breaking cryptosystems, i.e., receiving and understanding the message when you are not within the specific group of users allowed access to the message. The original message is referred to as a plaintext message or plaintext. The encrypted message is called a ciphertext, wherein encryption includes any means to convert plaintext into ciphertext. Decryption includes any means to convert ciphertext into plaintext, i.e., recover the original message. As illustrated in FIG. 1A, the plaintext message is encrypted to form a ciphertext. The ciphertext is then received and decrypted to recover the plaintext. While the terms plaintext and ciphertext generally refer to data, the concepts of encryption may be applied to any digital information, including audio and video data presented in digital form. While the description

of the invention provided herein uses the term plaintext and ciphertext consistent with the art of cryptography, these terms do not exclude other forms of digital communications.

[1029] A cryptosystem is based on secrets. A group of entities shares a secret if an entity outside this group cannot obtain the secret without significantly large amount of resources. This secret is said to serve as a security association between the groups of entities.

[1030] A cryptosystem may be a collection of algorithms, wherein each algorithm is labeled and the labels are called keys. A symmetric encryption system, often referred to as a cryptosystem, uses a same key (i.e., the secret key) to encrypt and decrypt a message. A symmetric encryption system 20 is illustrated in FIG. 1B, wherein both the encryption and decryption utilize a same private key.

[1031] In contrast, an asymmetric encryption system uses a first key (i.e., the public key) to encrypt a message and uses a different key (i.e., the private key) to decrypt it. FIG. 1C illustrates an asymmetric encryption system 30 wherein one key is provided for encryption and a second key for decryption. Asymmetric cryptosystems are also called public key cryptosystems. The public key is published and available for encrypting any message, however, only the private key may be used to decrypt the message encrypted with the public key.

[1032] A problem exists in symmetric cryptosystems in the secure provision of the secret key from a sender to a recipient. In one solution a courier may be used to provide the information, or, a more efficient and reliable solution may be to use a public key cryptosystem, such as a public-key cryptosystem defined by Rivest, Shamir, and Adleman (RSA) which is discussed hereinbelow. The RSA system is used in the popular security tool referred to as Pretty Good Privacy (PGP), which is further detailed hereinbelow. For instance, an originally recorded cryptosystem altered letters in a plaintext by shifting each letter by *n* in the alphabet, wherein *n* is a predetermined constant integer value. In such a scheme, an "A" is replaced with a "D," etc., wherein a given encryption scheme may incorporate several different values of *n*. In this encryption scheme "*n*" is the key. Intended recipients are provided the encryption scheme prior to receipt of a ciphertext. In this way, only those knowing the key should be able to decrypt the ciphertext to recover the plaintext. However, by calculating the key

with knowledge of encryption, unintended parties may be able to intercept and decrypt the ciphertext, creating a security problem.

[1033] More complicated and sophisticated cryptosystems employ strategic keys that are deter interception and decryption from unintended parties. A classic cryptosystem employs encryption functions E and decryption functions D such that:

$$D\_K(E\_K(P)) = P, \text{ for any plaintext } P. \quad (1)$$

[1034] In a public-key cryptosystem, E_K is easily computed from a known ``public key'' Y which in turn is computed from K. Y is published, so that anyone can encrypt messages. The decryption function D_K is computed from public key Y, but only with knowledge of a private key K. Without the private key K an unintended recipient may not decrypt the ciphertext so generated. In this way only the recipient who generated K can decrypt messages.

[1035] RSA is a public-key cryptosystem defined by Rivest, Shamir, and Adleman. As an example, consider plaintexts as positive integers up to 2^{512}. Keys are quadruples (*p,q,e,d*), with *p* given as a 256-bit prime number, *q* as a 258-bit prime number, and *d* and *e* large numbers with (*de* - 1) divisible by (*p*-1)(*q*-1). Further, define the encryption function as:

$$E\_K(P) = P^e \bmod pq, \; D\_K(C) = C^d \bmod pq. \quad (2)$$

[1036] While, E_K is easily computed from the pair (*pq,e*), there is no known simple way to compute D_K from the pair (*pq,e*). Therefore, the recipient that generates K can publish (*pq,e*). It is possible to send a secret message to the recipient, as he is the one able to read the message.

[1037] PGP combines features from symmetric and asymmetric encryption. FIGs. 1D and 1E illustrate a PGP cryptosystem 50, wherein a plaintext message is encrypted and recovered. In FIG. 1D, the plaintext message is compressed to save modem transmission time and disk space. Compression strengthens cryptographic security by adding another level of translation to the encrypting and decrypting processing. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby enhancing resistance to cryptanalysis. Note that one embodiment does not compress plaintext or other messages that are too short to compress or which don't compress well aren't compressed.

[1038] PGP then creates a *session key*, which is a one-time-only secret key. This key is a random number that may be generated from any random event(s), such as random movements of mouse and the keystrokes while typing. The session key works with a secure encryption algorithm to encrypt the plaintext, resulting in ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

[1039] For decryption, as illustrated in FIG. 1E, the recipient's copy of PGP uses a private key to recover the temporary session key, which PGP then uses to decrypt the conventionally encrypted ciphertext. The combination of encryption methods takes advantage of the convenience of public key encryption and the speed of symmetric encryption. Symmetric encryption is generally much faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. In combination, performance and key distribution are improved without any sacrifice in security.

[1040] A key is a value that works with a cryptographic algorithm to produce a specific ciphertext. Keys are basically very large numbers. Key size is measured in bits. In public key cryptography, security increases with key size, however, public key size and the symmetric encryption private key size are not generally related. While the public and private keys are mathematically related, a difficulty arises in deriving a private key given only a public key. Deriving the private key is possible given enough time and computing power, making the selection of key size an important security issue. The goal is to have a large key that is secure, while maintaining key size sufficiently small for quick processing. An additional consideration is the expected interceptor, specifically, what is the importance of a message to a third party, and how much resource does a third party have to decrypt.

[1041] Larger keys will be cryptographically secure for a longer period of time. Keys are stored in encrypted form. PGP specifically stores keys in two files; one for public keys and one for private keys. These files are called *keyrings*. In application, a PGP encryption system adds the public keys of target recipients to the sender's public keyring. The sender's private keys are stored on the sender's private keyring.

[1042] As discussed in the examples given hereinabove, the method of distributing the keys used for encryption and decryption can be complicated. The ``key exchange problem'' involves first ensuring that keys are exchanged such that both the sender and receiver can perform encryption and decryption, respectively, and for bi-directional communication, such that the sender and receiver can both encrypt and decrypt messages. Further, it is desired that key exchange be performed so as to preclude interception by a third unintended party. Finally, an additional consideration is authentication providing assurance to the receiver that a message was encrypted by an intended sender and not a third party. In a private key exchange system, the keys are exchanged secretly providing improved security upon successful key exchange and valid authentication. Note that the private key encryption scheme implicitly provides authentication. The underlying assumption in a private key cryptosystem is that only the intended sender will have the key capable of encrypting messages delivered to the intended receiver. While public-key cryptographic methods solve a critical aspect of the `key-exchange problem', specifically their resistance to analysis even with the presence a passive eavesdropper during exchange of keys, they do not solve all problems associated with key exchange. In particular, since the keys are considered `public knowledge,' (particularly with RSA) some other mechanism is desired to provide authentication, as possession of keys alone (sufficient to encrypt messages) is no evidence of a particular unique identity of the sender, nor is possession of a corresponding decryption key by itself enough to establish the identity of the recipient.

[1043] One solution is to develop a key distribution mechanism that assures that listed keys are actually those of the given entities, sometimes called a trusted authority, certificate authority, or third part escrow agent. The authority typically does not actually generate keys, but does ensure that the lists of keys and associated identities kept and advertised for reference by senders and receivers are correct and uncompromised. Another method relies on users to distribute and track each other's keys and trust in an informal, distributed fashion. Under RSA, if a user wishes to send evidence of their identity in addition to an encrypted message, a signature is encrypted with the private key. The receiver can use the RSA algorithm in reverse to verify that the information decrypts, such that only the sender could have encrypted the plaintext by use of

the secret key. Typically the encrypted `signature' is a `message digest' that comprises a unique mathematical `summary' of the secret message (if the signature were static across multiple messages, once known previous receivers could use it falsely). In this way, theoretically only the sender of the message could generate a valid signature for that message, thereby authenticating it for the receiver.

[1044] A message digest is often computed using a cryptographic hash function. A cryptographic hash function computes a value (with a fixed number of bits) from any input, regardless of the length of the input. One property of a cryptographic hash function is this: given an output value, it is computationally difficult to determine an input that will result in that output. An example of a cryptographic hash function is SHA-1 as described in "Secure Hash Standard," FIPS PUB 180-1, promulgated by the Federal Information Processing Standards Publications (FIPS PUBS) and issued by the National Institute of Standards and Technology.

[1045] FIG. 2 serves as an example of a communications system 100 that supports a number of users and is capable of implementing at least some aspects and embodiments of the invention. Any of a variety of algorithms and methods may be used to schedule transmissions in system 100. System 100 provides communication for a number of cells 102A through 102G, each of which is serviced by a corresponding base station 104A through 104G, respectively. In the exemplary embodiment, some of base stations 104 have multiple receive antennas and others have only one receive antenna. Similarly, some of base stations 104 have multiple transmit antennas, and others have single transmit antennas. There are no restrictions on the combinations of transmit antennas and receive antennas. Therefore, it is possible for a base station 104 to have multiple transmit antennas and a single receive antenna, or to have multiple receive antennas and a single transmit antenna, or to have both single or multiple transmit and receive antennas.

[1046] Terminals 106 in the coverage area may be fixed (i.e., stationary) or mobile. As shown in FIG. 2, various terminals 106 are dispersed throughout the system. Each terminal 106 communicates with at least one and possibly more base stations 104 on the downlink and uplink at any given moment depending on, for example, whether soft handoff is employed or whether the

terminal is designed and operated to (concurrently or sequentially) receive multiple transmissions from multiple base stations. Soft handoff in CDMA communications systems is well known in the art and is described in detail in U.S. Patent No. 5,101,501, entitled "METHOD AND SYSTEM FOR PROVIDING A SOFT HANDOFF IN A CDMA CELLULAR TELEPHONE SYSTEM," which is assigned to the assignee of the present invention.

[1047] The downlink refers to transmission from the base station to the terminal, and the uplink refers to transmission from the terminal to the base station. In the exemplary embodiment, some of terminals 106 have multiple receive antennas and others have only one receive antenna. In FIG. 2, base station 104A transmits data to terminals 106A and 106J on the downlink, base station 104B transmits data to terminals 106B and 106J, base station 104C transmits data to terminal 106C, and so on.

[1048] Increasing demand for wireless data transmission and the expansion of services available via wireless communication technology have led to the development of specific data services. One such service is referred to as High Data Rate (HDR). An exemplary HDR service is proposed in "EIA/TIA-IS856 cdma2000 High Rate Packet Data Air Interface Specification" referred to as "the HDR specification." HDR service is generally an overlay to a voice communication system that provides an efficient method of transmitting packets of data in a wireless communication system. As the amount of data transmitted and the number of transmissions increases, the limited bandwidth available for radio transmissions becomes a critical resource. There is a need, therefore, for an efficient and fair method of scheduling transmissions in a communication system that optimizes use of available bandwidth. In the exemplary embodiment, system 100 illustrated in FIG. 2 is consistent with a CDMA type system having HDR service.

[1049] According to one embodiment, the system 100 supports a high-speed multimedia broadcasting service referred to as High-Speed Broadcast Service (HSBS). An example application for HSBS is video streaming of movies, sports events, etc. The HSBS service is a packet data service based on the Internet Protocol (IP). According to the exemplary embodiment, a service provider indicates the availability of such high-speed broadcast service to the users. The users desiring the HSBS service subscribe to receive the service and may

discover the broadcast service schedule through advertisements, Short Management System (SMS), Wireless Application Protocol (WAP), etc. Mobile users are referred to as Mobile Stations (MSs). Base Stations (BSs) transmit HSBS related parameters in overhead messages. When an MS desires to receive the broadcast session, the MS reads the overhead messages and learns the appropriate configurations. The MS then tunes to the frequency containing the HSBS channel, and receives the broadcast service content.

[1050] The service being considered is a high-speed multimedia broadcasting service. This service is referred to as High-Speed Broadcast Service (HSBS) in this document. One such example is video streaming of movies, sports events, etc. This service will likely be a packet data service based on the Internet Protocol (IP).

[1051] The service provider will indicate the availability of such high-speed broadcast service to the users. The mobile station users who desire such service will subscribe to receive this service and may discover the broadcast service schedule through advertisements, SMS, WAP, etc. Base stations will transmit broadcast service related parameters in overhead messages. The mobiles that wish to listen to the broadcast session will read these messages to determine the appropriate configurations, tune to the frequency containing the high-speed broadcast channel, and start receiving the broadcast service content.

[1052] There are several possible subscription/revenue models for HSBS service, including free access, controlled access, and partially controlled access. For free access, no subscription is needed by the mobiles to receive the service. The BS broadcasts the content without encryption and interested mobiles can receive the content. The revenue for the service provider can be generated through advertisements that may also be transmitted in the broadcast channel. For example, upcoming movie-clips can be transmitted for which the studios will pay the service provider.

[1053] For controlled access, the MS users subscribe to the service and pay the corresponding fee to receive the broadcast service. Unsubscribed users are not able to receive the HSBS service. Controlled access can be achieved by encrypting the HSBS transmission/content so that only the subscribed users can decrypt the content. This may use over-the-air encryption key exchange

procedures. This scheme provides strong security and prevents theft-of-service.

[1054] A hybrid access scheme, referred to as partial controlled access, provides the HSBS service as a subscription-based service that is encrypted with intermittent unencrypted advertisement transmissions. These advertisements may be intended to encourage subscriptions to the encrypted HSBS service. Schedule of these unencrypted segments could be known to the MS through external means.

[1055] A wireless communication system 200 is illustrated in FIG. 3, wherein video and audio information is provided to Packetized Data Service Network (PDSN) 202 by a Content Server (CS) 201. The video and audio information may be from televised programming or a radio transmission. The information is provided as packetized data, such as in IP packets. The PDSN 202 processes the IP packets for distribution within an Access Network (AN). As illustrated the AN is defined as the portions of the system including a BS 204 in communication with multiple MS 206. The PDSN 202 is coupled to the BS 204. For HSBS service, the BS 204 receives the stream of information from the PDSN 202 and provides the information on a designated channel to subscribers within the system 200. To control the access, the content is encrypted by the CS 201 before being provided to the PDSN 202. The subscribed users are provided with the decryption key so that the IP packets can be decrypted.

[1056] FIG. 4 details an MS 300, similar to MS 206 of FIG. 3. The MS 300 has an antenna 302 coupled to receive circuitry 304. The MS 300 receives transmissions from a BS (not shown) similar to BS 204 of FIG. 3. The MS 300 includes a User Identification Module (UIM) 308 and a Mobile Equipment (ME) 306. The receive circuitry is coupled to the UIM 308 and the ME 306. The UIM 308 applies verification procedures for security of the HSBS transmission and provides various keys to the ME 306. The ME 306 may be coupled to processing unit 312. The ME 306 performs substantial processing, including, but not limited to, decryption of HSBS content streams. The ME 306 includes a memory storage unit, MEM 310. In the exemplary embodiment the data in the ME 306 processing (not shown) and the data in the ME memory storage unit, MEM 310 may be accessed easily by a non-subscriber by the use of limited resources, and therefore, the ME 306 is said to be insecure. Any information

passed to the ME 306 or processed by the ME 306 remains securely secret for only a short amount of time. It is therefore desired that any secret information, such as key(s), shared with the ME 306 be changed often.

[1057] The UIM 308 is trusted to store and process secret information (such as encryption keys) that should remain secret for a long time. As the UIM 308 is a secure unit, the secrets stored therein do not necessarily require the system to change the secret information often. The UIM 308 includes a processing unit referred to as a Secure UIM Processing Unit (SUPU) 316 and memory storage unit referred to as a Secure UIM Memory Unit (SUMU) 314 that is trusted to be secure. Within the UIM 308, SUMU 314 stores secret information in such a way that as to discourage unauthorized access to the information. If the secret information is obtained from the UIM 308, the access will require a significantly large amount of resources. Also within the UIM 308, the SUPU 316 performs computations on values that may be external to the UIM 308 and/or internal to the UIM 308. The results of the computation may be stored in the SUMU 314 or passed to the ME 306. The computations performed with the SUPU 316 can only be obtained from the UIM 308 by an entity with significantly large amount of resources. Similarly, outputs from the SUPU 316 that are designated to be stored within the SUMU 314 (but not output to the ME 306) are designed such that unauthorized interception requires significantly large amount of resources. In one embodiment, the UIM 308 is a stationary unit within the MS 300. Note that in addition to the secure memory and processing within the UIM 308, the UIM 308 may also include non-secure memory and processing (not shown) for storing information including telephone numbers, e-mail address information, web page or URL address information, and/or scheduling functions, etc.

[1058] Alternate embodiments may provide a removable and/or reprogrammable UIM. In the exemplary embodiment, the SUPU 316 does not have significant processing power for functions beyond security and key procedures, such as to allow encryption of the broadcast content of the HSBS. Alternate embodiments may implement a UIM having stronger processing power.

[1059] The UIM is associated with a particular user and is used primarily to verify that the MS 300 is entitled to the privileges afforded the user, such as access to the mobile phone network. Therefore, a user is associated with the

UIM 308 rather than an MS 300. The same user may be associated with multiple UIM 308.

[1060] The broadcast service faces a problem in determining how to distribute keys to subscribed users. To decrypt the broadcast content at a particular time, the ME must know the current decryption key. To avoid theft-of-service, the decryption key should be changed frequently, for example, every minute. These decryption keys are called Short-term Keys (SK). The SK is used to decrypt the broadcast content for a short-amount of time so the SK can be assumed to have some amount of intrinsic monetary value for a user. For example, this intrinsic monetary value may be a portion of the registration costs. Assume that the cost of a non-subscriber obtaining SK from the memory storage unit, MEM 310, of a subscriber exceeds the intrinsic monetary value of SK. That is, the cost of obtaining SK (illegitimately) exceeds the reward, so there is no benefit. Consequently, there is no need to protect SK in the memory storage unit, MEM 310. However, if a secret key has a lifetime longer than that of an SK, then the cost of obtaining this secret key (illegitimately) is less than the reward. In this situation, there is a benefit in obtaining such a key from the memory storage unit, MEM 310. Hence, ideally the memory storage unit, MEM 310 will not store secrets with a lifetime longer than that of an SK.

[1061] The channels used by the CS (not shown) to distribute the SK to the various subscriber units are considered insecure. Therefore, when distributing a given SK, the CS desires to use a technique that hides the value of the SK from non-subscribed users. Furthermore, the CS distributes the SK to each of a potentially large number of subscribers for processing in respective MEs within a relatively short timeframe. Known secure methods of key transmission are slow and require transmission of a large number of keys, and are generally not feasible for the desired criteria. The exemplary embodiment is a feasible method of distributing decryption keys to a large set of subscribers within a small time-frame in such a way that non-subscribers cannot obtain the decryption keys.

[1062] In the exemplary embodiment, the MS 300 supports HSBS in a wireless communication system. To obtain access to HSBS, the user must register and then subscribe to the service. Once the subscription is enabled, the various keys are updated periodically. In the registration process the CS

and UIM 308 agree on a Registration Key (RK) that serves as a security association between the user and the CS. The CS may then send the UIM further secret information encrypted with the RK. The RK is kept as a secret in the UIM 308, and is unique to a given UIM, i.e., each user is assigned a different RK. The registration process alone does not give the user access to HSBS. As stated hereinabove, after registration the user subscribes to the service. In the subscription process the CS sends the UIM 308 the value of a common Broadcast Access Key (BAK). The CS sends the MS 300, and specifically UIM 308, the value of BAK encrypted using the RK unique to UIM 308. The UIM 308 is able to recover the value of the original BAK from the encrypted version using the RK. The BAK serves as a security association between the CS and the group of subscribed users. The CS then broadcasts data called SK Information (SKI) that is combined with the BAK in the UIM 308 to derive SK. The UIM 308 then passes SK to the ME 306. In this way, the CS can efficiently distribute new values of SK to the ME of subscribed users.

[1063] The following paragraphs discuss the registration process in more detail. When a user registers with a given CS, the UIM 308 and the CS (not shown) set-up a security association. That is, the UIM 308 and the CS agree on a secret key RK. The RK is unique to each UIM 308, although if a user has multiple UIMs then these UIMs may share the same RK dependent on the policies of the CS. This registration may occur when the user subscribes to a broadcast channel offered by the CS or may occur prior to subscription. A single CS may offer multiple broadcast channels. The CS may choose to associate the user with the same RK for all channels or require the user to register for each channel and associate the same user with different RKs on different channels. Multiple CSs may choose to use the same registration keys or require the user to register and obtain a different RK for each CS.

[1064] Two common scenarios for setting up this security association include the Authenticated Key Agreement (AKA) method (as used in 3GPP) and the Internet Key Exchange (IKE) method as used in IPsec. In either case the UIM memory unit SUMU 314 contains a secret key referred to as the A-key. As an example, the AKA method is described. In the AKA method the A-key is a secret known only to the UIM and a trusted third party (TTP): the TTP may consist of more than one entity. The TTP is typically the mobile service provider

with whom the user is registered. All communication between the CS and TTP is secure, and the CS trusts that the TTP will not assist unauthorized access to the broadcast service. When the user registers, the CS informs the TTP that the user wishes to register for the service and provides verification of the user's request. The TTP uses a function (similar to a cryptographic hash function) to compute the RK from the A-key and additional data called Registration Key Information (RKI). The TTP passes RK, RKI to the CS over a secure channel along with other data not relevant to this submission. The CS sends RKI to the MS 300. The receiver circuitry 304 passes RKI to the UIM 308 and possibly passes RKI to the ME 306. The UIM 308 computes RK from RKI and the A-key that is stored in the UIM memory unit SUMU 314. The RK is stored in the UIM memory unit SUMU 314 and is not provided directly to the ME 306. Alternate embodiments may use an IKE scenario or some other method to establish the RK. The RK serves as the security association between the CS and UIM 308.

[1065] In the AKA method, the RK is a secret shared between the CS, UIM and TTP. Therefore, as used herein, the AKA method implies that any security association between the CS and UIM implicitly includes the TTP. The inclusion of the TTP in any security association is not considered a breach of security, as the CS trusts the TTP not to assist in unauthorized access to the broadcast channel. As stated hereinabove, if a key is shared with the ME 306, it is desirable to change that key often. This is due to the risk of a non-subscriber accessing information stored in memory storage unit, MEM 310 and thus allowing access to a controlled or partially controlled service. The ME 306 stores SK (key information used for decrypting broadcast content) in memory storage unit, MEM 310. The CS must send sufficient information for subscribed users to compute SK. If the ME 306 of a subscribed user could compute SK from this information, then additional information required to compute SK cannot be secret. In this case, assume that the ME 306 of a non-subscribed user could also compute SK from this information. Hence, the value of SK must be computed in the SUPU 316, using a secret key shared by the CS and SUMU 314. The CS and SUMU 314 share the value of RK, however each user has a unique value of RK. There is insufficient time for the CS to encrypt SK with every value of RK and transmit these encrypted values to each subscribed user. Some other technique is required.

[1066] The following paragraphs discuss the subscription process in more detail. To ensure the efficient distribution of the security information SK, the CS periodically distributes a common Broadcast Access Key (BAK) to each subscriber UIM 308. For each subscriber the CS encrypts BAK using the corresponding RK to obtain a value called BAKI (BAK Information). The CS sends the corresponding BAKI to MS 300 of the subscribed user. For example, BAK may be transmitted as an IP packet encrypted using the RK corresponding to each MS. In the exemplary embodiment, the BAKI is an IPSec packet. In the exemplary embodiment, BAKI is an IPSec packet containing BAK that is encrypted using RK as the key. Since RK is a per-user key, the CS must send the BAK to each subscriber individually; thus, the BAK is not sent over the broadcast channel. The MS 300 passes the BAKI to the UIM 308. The SUPU 316 computes BAK using the value of RK stored in SUMU 314 and the value of BAKI. The value of BAK is then stored in the SUMU. In the exemplary embodiment, the BAKI contains a Security Parameter Index (SPI) value instructing the MS 300 to pass BAKI to the UIM 308, and instructing the UIM 308 to use the RK for decrypting the BAKI.

[1067] The period for updating the BAK is desired to be sufficient to allow the CS to send the BAK to each subscriber individually, without incurring significant overhead. Since the ME 306 is not trusted to keep secrets for a long time, the UIM 308 does not provide the BAK to the ME 306. The BAK serves as the security association between the CS and the group of subscribers of HSBS service.

[1068] The following paragraph discusses how the SK is updated following a successful subscription process. Within each period for updating the BAK, a short-term interval is provided during which SK is distributed on a broadcast channel. The CS uses a cryptographic function to determine two values SK and SKI (SK Information) such that SK can be determined from BAK and SKI. For example, SKI may be the encryption of SK using BAK as the key. In the exemplary embodiment, SKI is an IPSec packet containing SK that is encrypted using BAK as the key. Alternatively, SK may be the result of applying a cryptographic hash function to the concatenation of the blocks SKI and BAK.

[1069] Some portion of SKI may be predictable. For example, a portion of SKI may be derived from the system time during which this SKI is valid. This

portion, denoted SKI_A, need not be transmitted to the MS 300 as part of the broadcast service. The remainder of SKI, SKI_B may be unpredictable. The SKI_B need not be transmitted to the MS 300 as part of the broadcast service. The MS 300 reconstructs SKI from SKI_A and SKI_B and provides SKI to UIM 308. The SKI may be reconstructed within the UIM 308. The value of SKI must change for each new SK. Thus, either SKI_A and/or SKI_B must change when computing a new SK. The CS sends SKI_B to BS for broadcast transmission. The BS broadcasts SKI_B, which is detected by the antenna 302 and passed to the receive circuitry 304. Receive circuitry 304 provides SKI_B to the MS 300, wherein the MS 300 reconstructs SKI. The MS 300 provides SKI to UIM 308, wherein the UIM 308 obtains the SK using the BAK stored in SUMU 314. The SK is then provided by UIM 308 to ME 306. The ME 306 stores the SK in memory storage unit, MEM 310. The ME 306 uses the SK to decrypt broadcast transmissions received from the CS.

[1070] In the exemplary embodiment, the SKI also contains a Security Parameter Index (SPI) value instructing the MS 300 to pass SKI to the UIM 308, and instructing the UIM 308 to use the BAK for decrypting the SKI. After decryption, the UIM 308 passes the SK to the ME 306, wherein ME 306 uses the SK to decrypt broadcast content.

[1071] The CS and BS agree on some criteria for when SKI_B is to be transmitted. The CS may desire to reduce the intrinsic monetary value in each SK by changing SK frequently. In this situation, the desire to change SKI_B data is balanced against optimizing available bandwidth. The SKI_B may be transmitted on a channel other than the broadcast channel. When a user "tunes" to the broadcast channel, the receive circuitry 304 obtains information for locating the broadcast channel from a "control channel." It may be desirable to allow quick access when a user "tunes" to the broadcast channel. This requires the ME 306 to obtain SKI within a short amount of time. The ME 306 will already know SKI_A, however, the BS must provide SKI_B to ME 300 within this short amount of time. For example, the BS may frequently transmit SKI_B on the control channel, (along with the information for locating the broadcast channel), or frequently transmit SKI_B on the broadcast channel. The more often that the BS "refreshes" the value of SKI_B, the faster the MS 300 can access the broadcast message. The desire to refresh SKI_B data is balanced

against optimizing available bandwidth, as transmitting SKI_B data too frequently may use an unacceptable amount of bandwidth in the control channel or broadcast channel.

[1072] This paragraph discusses the encryption and transmission of the broadcast content. The CS encrypts the broadcast content using the current SK. The exemplary embodiment employs an encryption algorithm such as the Advanced Encryption Standard (AES)h Cipher Algorithm. In the exemplary embodiment, the encrypted content is then transported by an IPsec packet according to the Encapsulating Security Payload (ESP) transport mode. The IPsec packet also contains an SPI value that instructs the ME 306 to use the current SK to decrypt received broadcast content. The encrypted content is sent via the broadcast channel.

[1073] Receive circuitry 304 provides the RKI and BAKI directly to the UIM 308. Further, receive circuitry 304 provides the SKI_B to an appropriate part of the MS 300 where it is combined with SKI_A to obtain SKI. The SKI is provided to the UIM 308 by the relevant part of the MS 300. The UIM 308 computes RK from the RKI and A-key, decrypts the BAKI using the RK to obtain BAK, and computes the SK using the SKI and BAK, to generate an SK for use by the ME 306. The ME 306 decrypts the broadcast content using the SK. The UIM 308 of the exemplary embodiment is not sufficiently powerful for decryption of broadcast content in real time, and, therefore, SK is passed to the ME 306 for decrypting the broadcast content.

[1074] FIG. 5 illustrates the transmission and processing of keys RK, BAK and SK according to the exemplary embodiment. As illustrated, at registration the MS 300 receives the RKI and passes it to UIM 308, wherein the SUPU 316 computes RK using RKI and the A-key, and stores the RK in UIM memory storage SUMU 314. The MS 300 periodically receives the BAKI that contains BAK encrypted using the RK value specific to UIM 308. The encrypted BAKI is decrypted by SUPU 316 to recover the BAK, which is stored in UIM memory storage SUMU 314. The MS 300 further periodically receives an SKI_B that it combines with SKI_A to form SKI. The SUPU 316 computes SK from SKI and BAK. The SK is provided to ME 306 for decrypting broadcast content.

[1075] In the exemplary embodiment the CS keys are not necessarily encrypted and transmitted to the MSs; the CS may use an alternative method.

The key information generated by the CS for transmission to each MS provides sufficient information for the MS to calculate the key. As illustrated in the system 350 of FIG. 6, the RK is generated by the CS, but RK Information (RKI) is transmitted to the MS. The CS sends information sufficient for the UIM to derive the RK, wherein a predetermined function is used to derive the RK from transmitted information from the CS. The RKI contains sufficient information for the MS to determine the original RK from the A_key and other values, such as system time, using a predetermined public function labeled d1, wherein:

[1076] $$RK = d1(A\text{-}key, RKI). \quad (3)$$

[1077] In the exemplary embodiment, the function d1 defines a cryptographic-type function. According to one embodiment, RK is determined as:

[1078] $$RK = SHA'(A\text{-}key \,||\, RKI), \quad (4)$$

[1079] wherein "||" denotes the concatenation of the blocks containing A-key and RKI, and SHA'(X) denotes the last 128-bits of output of the Secure Hash Algorithm SHA-1 given the input X. In an alternative embodiment, RK is determined as:

[1080] $$RK = AES(A\text{-}key,RKI), \quad (5)$$

[1081] wherein AES(X,Y) denotes the encryption of the 128-bit block RKI using the 128-bit A-key. In a further embodiment based on the AKA protocol, RK is determined as the output of the 3GPP key generation function *f3*, wherein RKI includes the value of RAND and appropriate values of AMF and SQN as defined by the standard.

[1082] The BAK is treated in a different manner because multiple users having different values of RK must compute the same value of BAK. The CS may use any technique to determine BAK. However, the value of BAKI associated with a particular UIM 308 must be the encryption of BAK under the unique RK associated with that UIM 308. The SUPU 316 decrypts BAKI using RK stored in the SUMU 314 according to the function labeled d2, according to:

[1083] $$BAK = d2(BAKI, RK). \quad (9)$$

[1084] In an alternate embodiment, the CS may compute BAKI by applying a decryption process to BAK using RK, and the SUPU 316 obtains BAK by applying the encryption process to BAKI using RK. This is considered equivalent to the CS encrypting BAK and the SUPU 316 decrypting BAKI.

Alternate embodiments may implement any number of key combinations in addition to or in place of those illustrated in FIG. 6.

[1085] The SK is treated in a similar manner to RK. First SKI is derived from the SKI_A and SKI_B (SKI_B is the information transmitted from CS to MS). Then a predetermined function labeled d3 is used to derive the SK from SKI and BAK (stored in the SUMU 314), according to:

[1086] $$SK = d3(BAK, SKI), \quad (6)$$

[1087] In one embodiment, the function d3 defines a cryptographic-type function. In an exemplary embodiment, SK is computed as:

[1088] $$SK = SHA(BAK \,||\, SKI), \quad (7)$$

[1089] while in another embodiment, SK is computed as

[1090] $$SK = AES(BAK, SKI). \quad (8)$$

[1091] A method of providing the security for a broadcast message is illustrated in FIGs. 7A-7D. FIG. 7A illustrates a registration process 400 wherein a subscriber negotiates registration with the CS at step 402. The registration at step 404 provides the UIM a unique RK. The UIM stores the RK in a Secure Memory Unit (SUMU) at step 406. FIG. 7B illustrates subscription processing 420 between a CS and a MS. At step 422 the CS generates a BAK for a BAK time period T1. The BAK is valid throughout the BAK time period T1, wherein the BAK is periodically updated. At step 424 the CS authorizes the UIM to have access to the Broadcast Content (BC) during the BAK timer period T1. At step 426 the CS encrypts the BAK using each individual RK for each subscriber. The encrypted BAK is referred to as the BAKI. The CS then transmits the BAKI to the UIM at step 428. The UIM receives the BAKI and performs decryption using the RK at step 430. The decrypted BAKI results in the originally generated BAK. The UIM stores the BAK n a SUMU at step 432. The UIM then receives the broadcast session and is able to access the BC by applying the BAK to decryption of the encrypted broadcast (EBC).

[1092] FIG. 7C illustrates a method of updating keys for security encryption in a wireless communication system supporting broadcast service. The method 440 implements time periods as given in FIG. 7E. The BAK is updated periodically having a time period T1. A timer t1 is initiated when BAK is calculated and times out at T1. A variable is used for calculating the SK referred to as SK_RAND, which is updated periodically having a time period T2.

A timer t2 is initiated when the SK_RAND is generated and times out at T2. In one embodiment, the SK is further updated periodically having a period of T3. A timer t3 is initiated when each SK is generated and time out at time T3. The SK_RAND is generated at the CS and provided periodically to the MS. The MS and the CS use SK_RAND to generate the SK, as detailed hereinbelow.

[1093] A first timer t1 is reset when the applicable value of BAK is updated. The length of time between two BAK updates is the BAK update period. In the exemplary embodiment the BAK update period is a month, however, alternate embodiments may implement any time period desired for optimum operation of the system, or to satisfy a variety of system criteria.

[1094] Continuing with FIG. 7C, the method 440 initializes the timer t2 at step 442 to start the SK_REG time period T2. The CS generates SK_RAND and provides the value to transmit circuitry for transmission throughout the system at step 444. The timer t3 is initialized at step 446 to start the SK time period T3. The CS then encrypts the BC using the current SK at step 448. The encrypted product is the EBC, wherein the CS provides the EBC to transmit circuitry for transmission in the system. If the timer t2 has expired at decision diamond 450, processing returns to step 442. While t2 is less than T2, if the timer t3 has expired at decision diamond 452, processing returns to step 446; else processing returns to 450.

[1095] FIG. 7D illustrates the operation of the MS accessing a broadcast service. The method 460 first synchronizes the timers t2 and t3 with the values at the CS at step 462. The UIM of the MS receives the SK_RAND generated by the CS at step 464. At step 466 the UIM generates the SK using the SK_RAND, BAK, and a time measurement. The UIM passes the SK to the ME of the MS. The UIM then decrypts the received EBC using the SK to extract the original BC at step 468. When the timer t2 expires at step 470 processing returns to step 462. While the timer t2 is less than T2, if the timer t3 expires at step 472, the timer t3 is initialized at step 474 and returns to 466.

[1096] When the user subscribes to the broadcast service for a particular BAK update period, the CS sends the appropriate information BAKI (corresponding to the BAK encrypted with the RK). This typically occurs prior to the beginning of this BAK update period or when the MS first tunes to the broadcast channel during this BAK update period. This may be initiated by the

MS or CS according to a variety of criteria. Multiple BAKI may be transmitted and decrypted simultaneously.

[1097] Note that when expiration of the BAK update period is imminent, the MS may request the updated BAK from the CS if the MS has subscribed for the next BAK update period. In an alternate embodiment the first timer t1 is used by the CS, where upon expiration of the timer, i.e., satisfaction of the BAK update period, the CS transmits the BAK.

[1098] Note that it is possible for a user to receive a BAK during a BAK update period, wherein, for example, a subscriber joins the service mid-month when the BAK updates are performed monthly. Additionally, the time periods for BAK and SK updates may be synchronized, such that all subscribers are updated at a given time.

[1099] FIG. 8A illustrates the registration process in a wireless communication system 500 according to the exemplary embodiment. The CS 502 negotiates with each subscriber, i.e., MS 512, to generate a specific RK to each of the subscribers. The RK is provided to the SUMU unit within the UIM of each MS. As illustrated, the CS 502 generates RK_1 which is stored in $SUMU_1$ 510 within UIM_1 512. Similarly, the CS 502 generates RK_2 and RK_N which are stored in $SUMU_2$ 520 within UIM_2 522 and $SUMU_N$ 530 within UIM_N 532, respectively.

[1100] FIG. 8B illustrates the subscription process in the system 500. The CS 502 further includes multiple encoders 504. Each of the encoders 504 receives one of the unique RKs and the BAK value generated in the CS 502. The output of each encoder 504 is a BAKI encoded specifically for a subscriber. The BAKI is received at the UIM of each MS, such as UIM_1 512. Each UIM includes a SUPU and a SUMU, such as $SUPU_1$ 514 and $SUMU_1$ 510 of UIM_1 512. The SUPU includes a decoder, such as decoder 516 that recovers the BAK by application of the RK of the UIM. The process is repeated at each subscriber.

[1101] Key management and updates are illustrated in FIG. 8C, wherein the CS applies a function 508 to generate a value of SK_RAND, which is an interim value used by the CS and MS to calculate SK. Specifically, the function 508 applies the BAK value, the SK_RAND and a time factor. While the embodiment illustrated in FIG. 8C applies a timer to determine when to update the SK,

alternate embodiments may use alternate measures to provide periodic updates, for example occurrence of an error or other event. The CS provides the SK_RAND value to each of the subscribers, wherein a function 518 resident in each UIM applies the same function as in function 508 of the CS. The function 518 operates on the SK_RAND, BAK and a timer value to generate a SK that is stored in a memory location in the ME, such as MEM_1 542 of ME_1 540.

[1102] FIG. 8D illustrates the processing of BC after registration and subscription. The CS 502 includes an encoder 560 that encodes the BC using the current SK to generate the EBC. The EBC is then transmitted to the subscribers. Each MS includes an encoder, such as encoder 544, that extracts the BC from the EBC using the SK.

[1103] While the present invention has been described with respect to an exemplary embodiment of a wireless communication system supporting a uni-directional broadcast service, the encryption methods and key management described hereinabove is further applicable to other data processing systems, including a multi-cast type broadcast system. Still further, application of the present invention to any data processing system wherein multiple subscribers access a single transmission of secure information through an insecure channel.

[1104] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[1105] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as

hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[1106] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[1107] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[1108] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to

other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

[1109] WHAT IS CLAIMED IS:

CLAIMS

1. A method for secure transmissions, the method comprising:
determining a registration key specific to a participant in a transmission;
determining a first key;
encrypting the first key with the registration key;
determining a second key;
encrypting the second key with the first key; and
updating the first and second keys.

2. The method as in claim 1, wherein updating further comprises:
updating the first key according to a first time period; and
updating the second key according to a second time period, wherein the second time period is less than the first time period.

3. The method as in claim 2, wherein updating further comprises:
encrypting an updated first key with the registration key ; and
encrypting an updated second key with the updated first key.

4. The method as in claim 2, further comprising:
encrypting a broadcast stream of information using the second key; and
transmitting the encrypted broadcast stream of information.

5. The method as in claim 4, wherein the broadcast stream of information comprises video information.

6. The method as in claim 4, wherein the broadcast stream of information comprises Internet Protocol packets.

7. The method as in claim 3, further comprising:
calculating a registration key information message; and
transmitting the registration key information message.

8. The method as in claim 7, further comprising:
calculating a first key information message corresponding to the updated and encrypted first key; and
transmitting the first key information message.

9. The method as in claim 8, further comprising:
calculating a second key information message corresponding to the updated and encrypted second key; and
transmitting the second key information message.

10. The method as in claim 1, further comprising:
transmitting the encrypted first key; and
transmitting the encrypted second key.

11. A method for secure reception of a transmission, the method comprising:
receiving a registration key specific to a participant in a transmission;
receiving a first key;
decrypting the first key with the registration key;
receiving a second key;
decrypting the second key with the first key;
receiving a broadcast stream of information; and
decrypting the broadcast stream of information using the second key.

12. The method as in claim 11, further comprising:
storing the first key in a secure memory storage unit; and
storing the second key in a memory storage unit.

13. The method as in claim 11, further comprising:
recovering the first key from a first key information message; and
recovering the second key from a second key information message.

14. The method as in claim 11, further comprising:
updating the first key according to a first time period; and
updating the second key according to a second time period.

15. In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:
a receive circuitry;
a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:
processing unit operative to decrypt key information;
memory storage unit for storing a registration key; and
a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message.

16. The infrastructure element as in claim 15, wherein the short-time key is processed by the user identification unit and passed to the mobile equipment unit.

17. The infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit.

18. The infrastructure element as in claim 15, wherein the memory storage unit stores a broadcast access key, and wherein the processing unit decrypts the short-time key using the broadcast access key.

19. The infrastructure element as in claim 18, wherein the short-time key is updated at a first frequency.

20. The infrastructure element as in claim 19, wherein the broadcast access key is updated at a second frequency less than the first frequency.

21. The infrastructure element as in claim 15, wherein the broadcast service option is a video service.

22. A wireless communication system, comprising:
means for determining a registration key specific to a participant in a transmission;

means for determining a first key;

means for encrypting the first key with the registration key;

means for determining a second key;

means for encrypting the second key with the first key; and

means for updating the first and second keys.

23. An infrastructure element, comprising:

means for receiving a registration key specific to a participant in a transmission;

means for receiving a first key;

means for decrypting the first key with the registration key;

means for receiving a second key;

means for decrypting the second key with the first key;

means for receiving a broadcast stream of information; and

means for decrypting the broadcast stream of information using the second key.

24. A digital signal storage device, comprising:

first set of instructions for receiving a registration key specific to a participant in a transmission;

second set of instructions for receiving a first key;

third set of instructions for decrypting the first key with the registration key;

fourth set of instructions for receiving a second key;

fifth set of instructions for decrypting the second key with the first key;

sixth set of instructions for receiving a broadcast stream of information; and

seventh set of instructions for decrypting the broadcast stream of information using the second key.

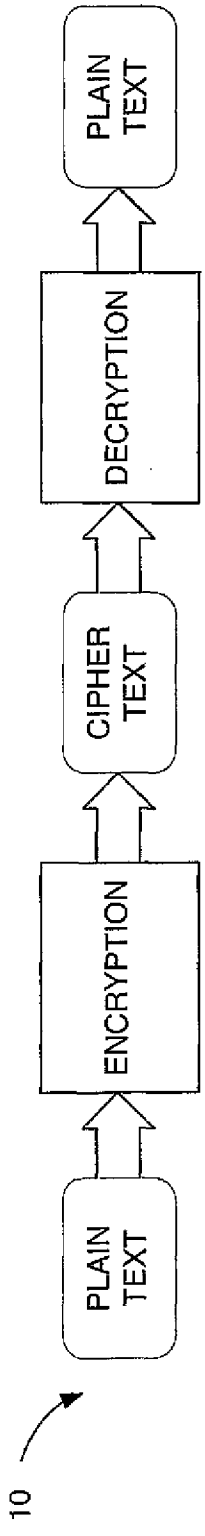


FIG. 1A

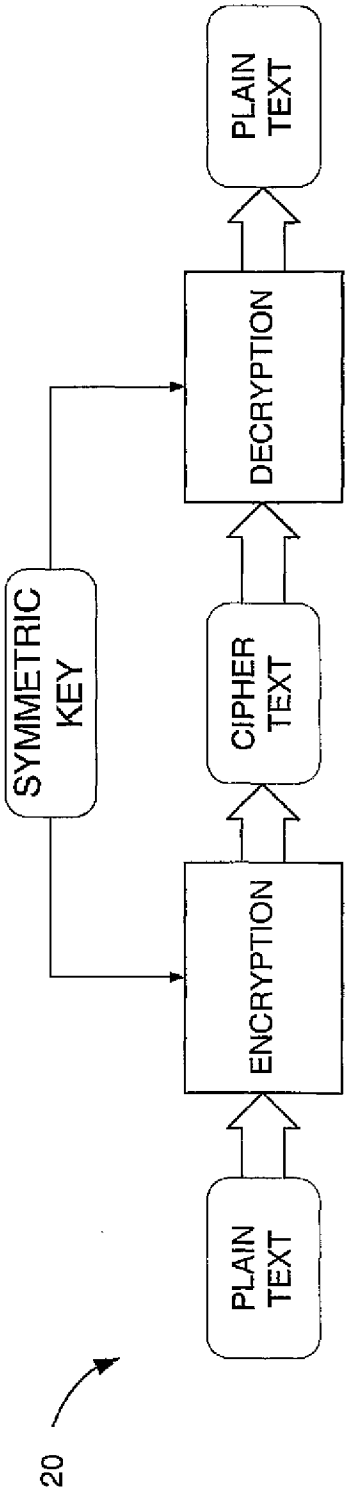


FIG. 1B

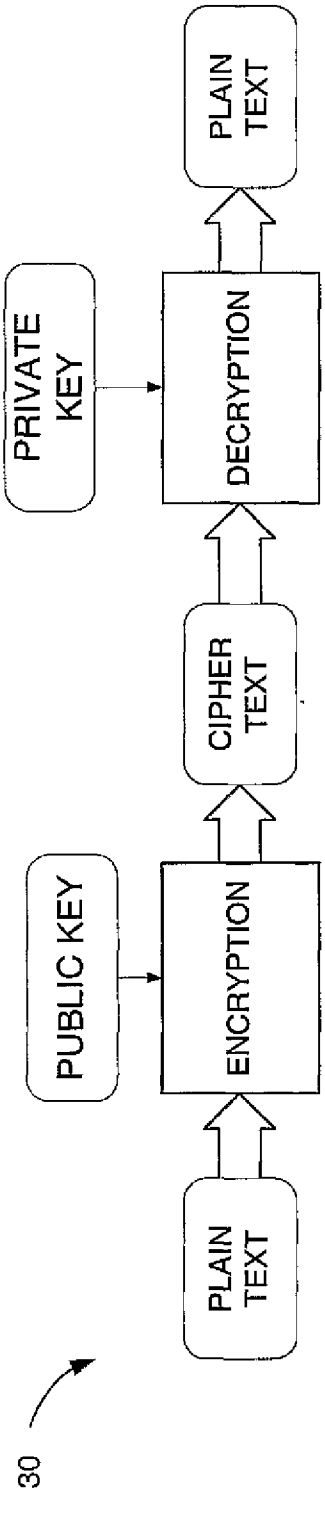


FIG. 1C

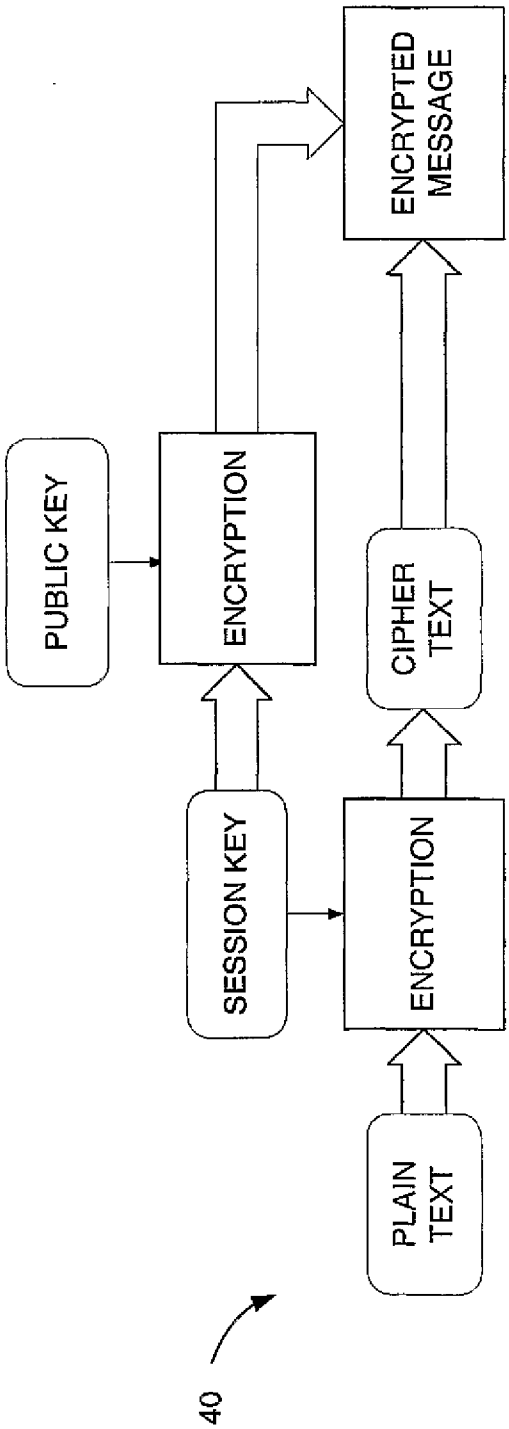

ENCRYPTED MESSAGE
PUBLIC KEY
ENCRYPTION
CIPHER TEXT
SESSION KEY
ENCRYPTION
PLAIN TEXT
40

FIG. 1D

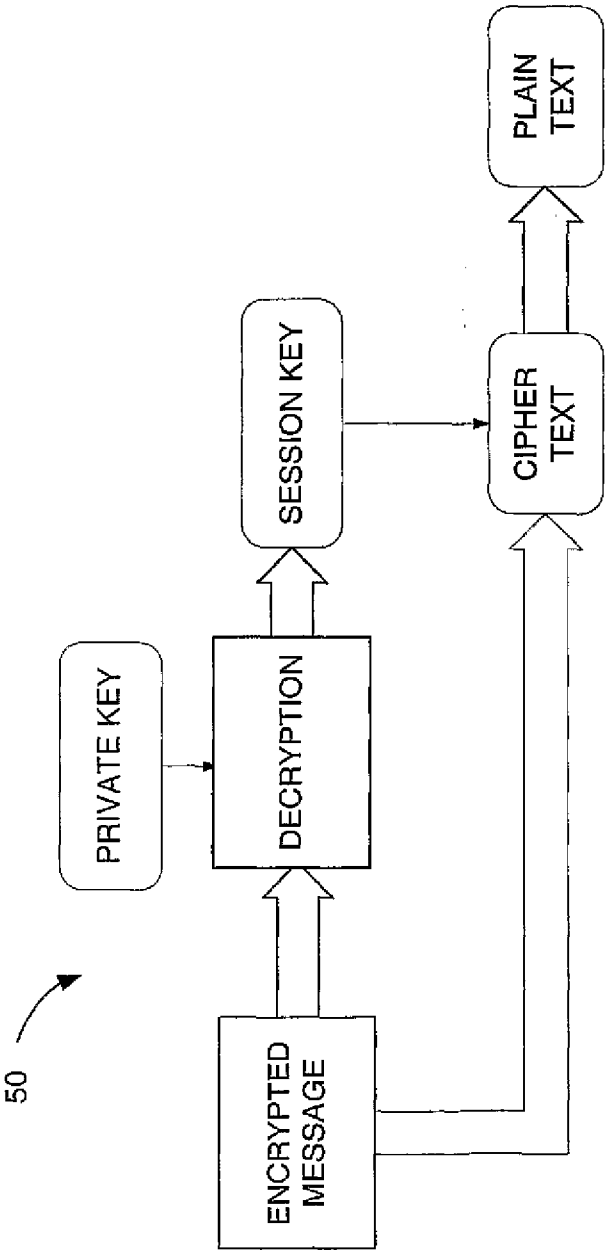

50
ENCRYPTED MESSAGE
PRIVATE KEY
DECRYPTION
SESSION KEY
CIPHER TEXT
PLAIN TEXT

FIG. 1E

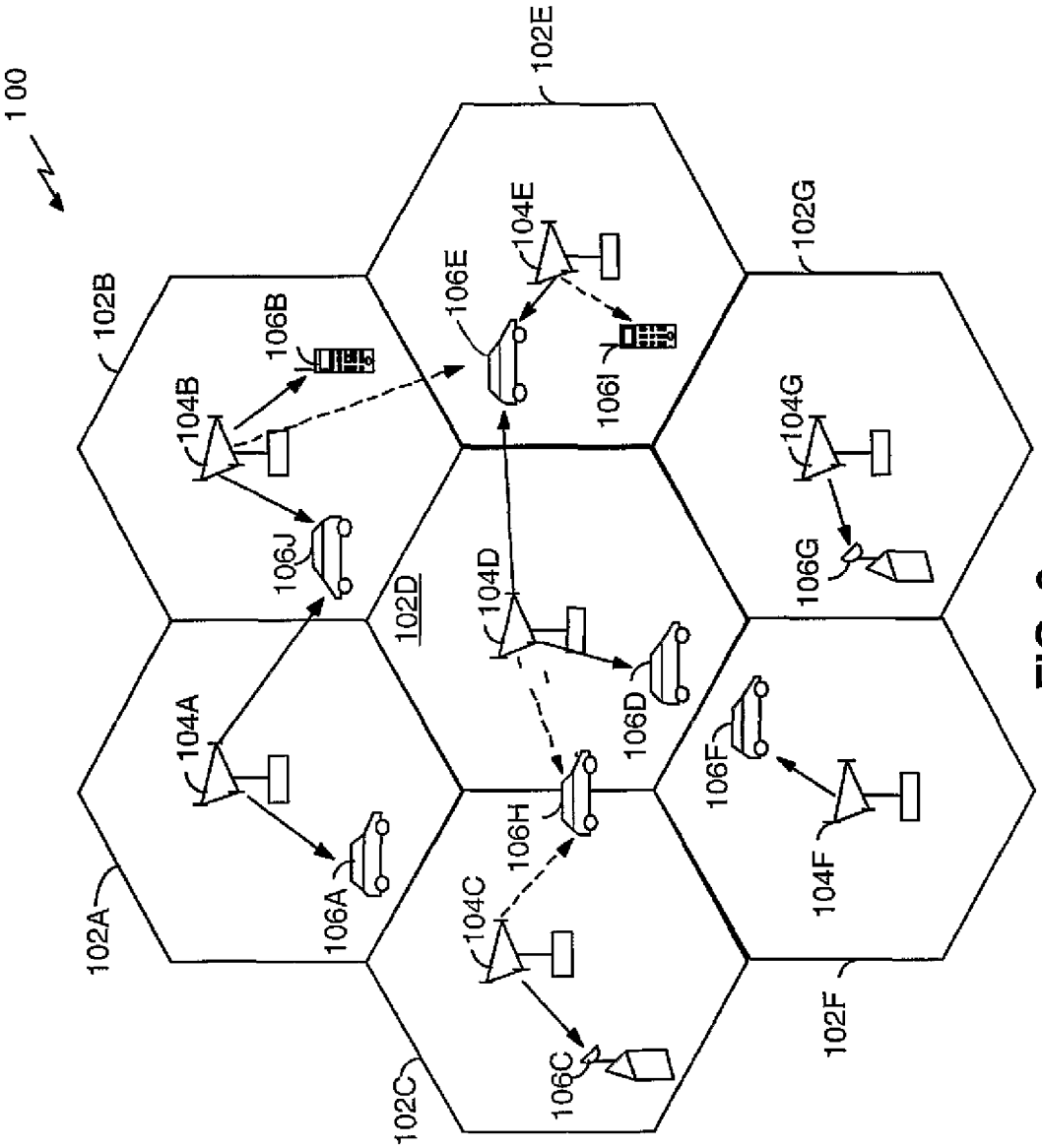

100
102A
102B
102C
102D
102E
102F
102G
104A
104B
104C
104D
104E
104F
104G
106A
106B
106C
106D
106E
106F
106G
106H
106I
106J

FIG. 2

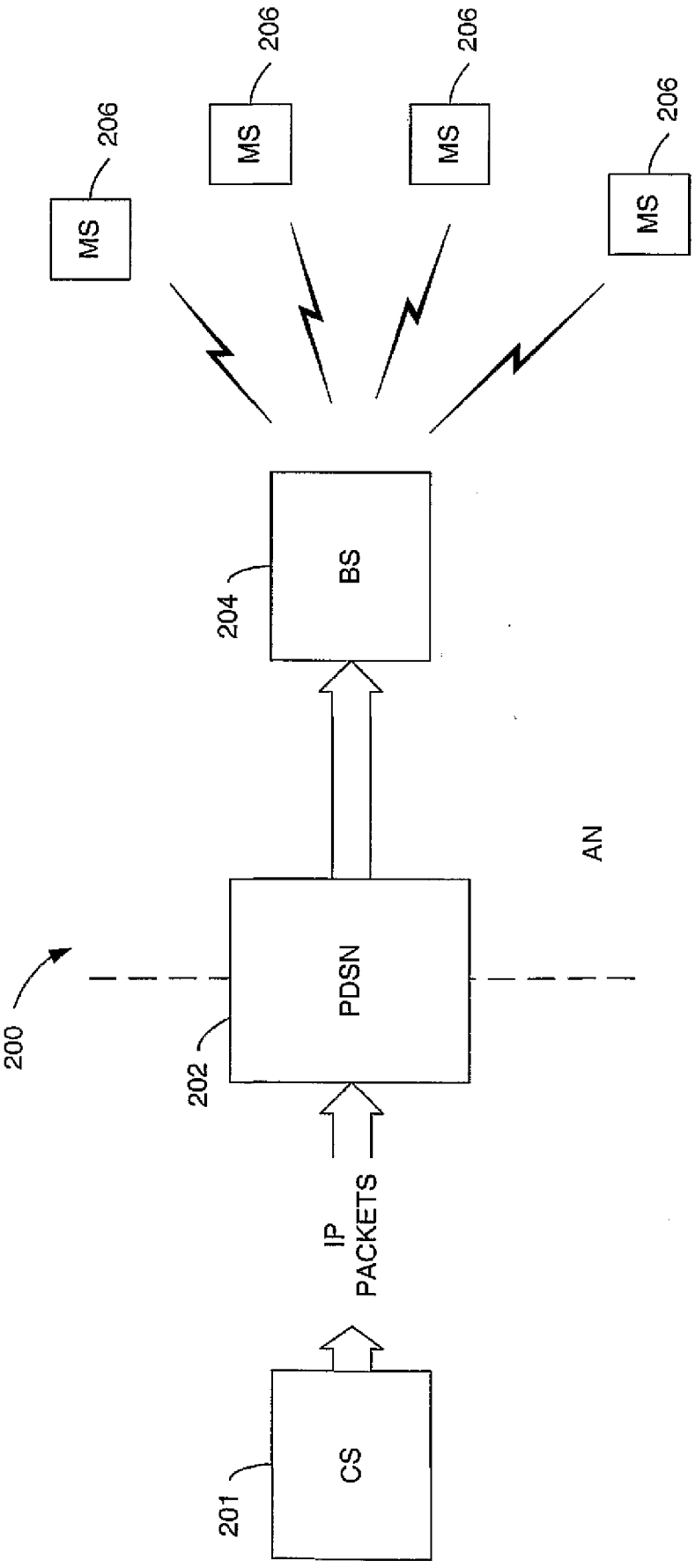


FIG. 3

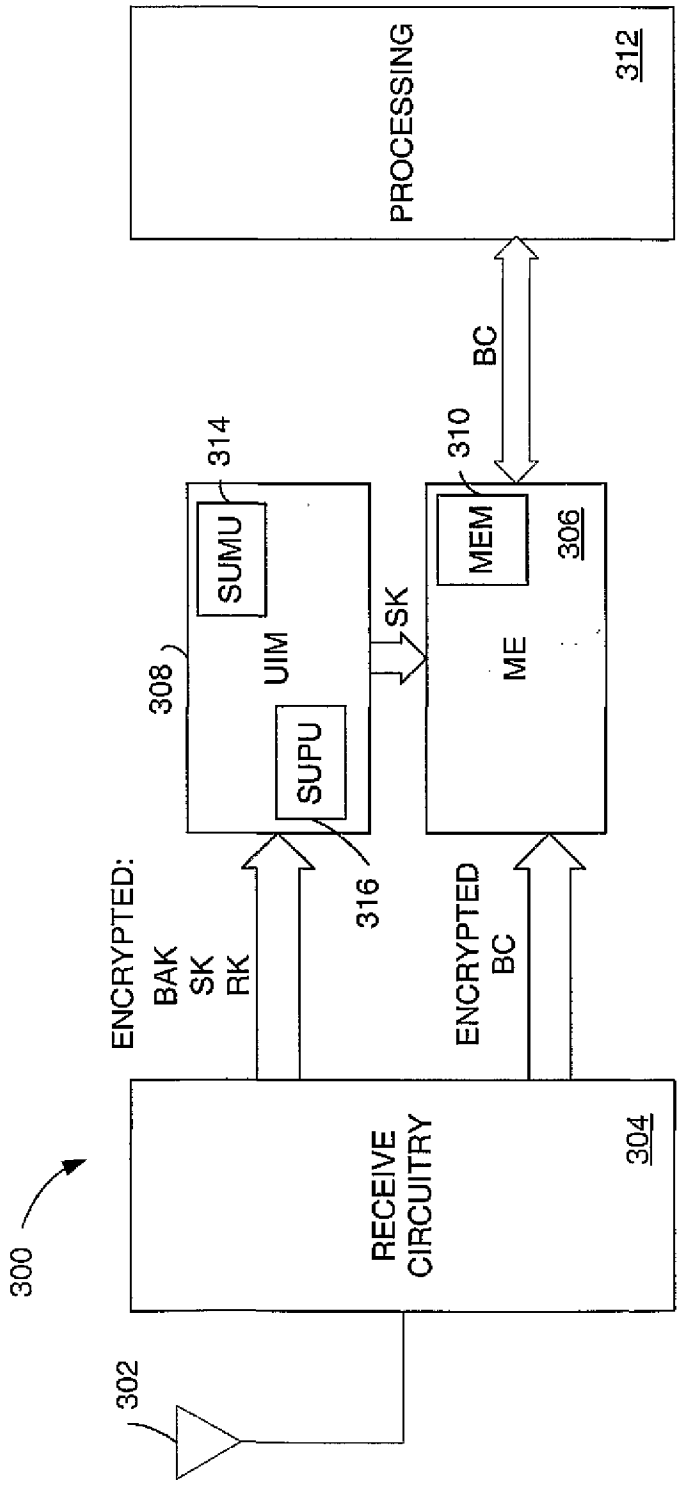

PROCESSING
312
BC
314
310
SUMU
MEM
306
308
UIM
SK
ME
SUPU
316
ENCRYPTED:
BAK
SK
RK
ENCRYPTED
BC
RECEIVE
CIRCUITRY
304
300
302

FIG. 4

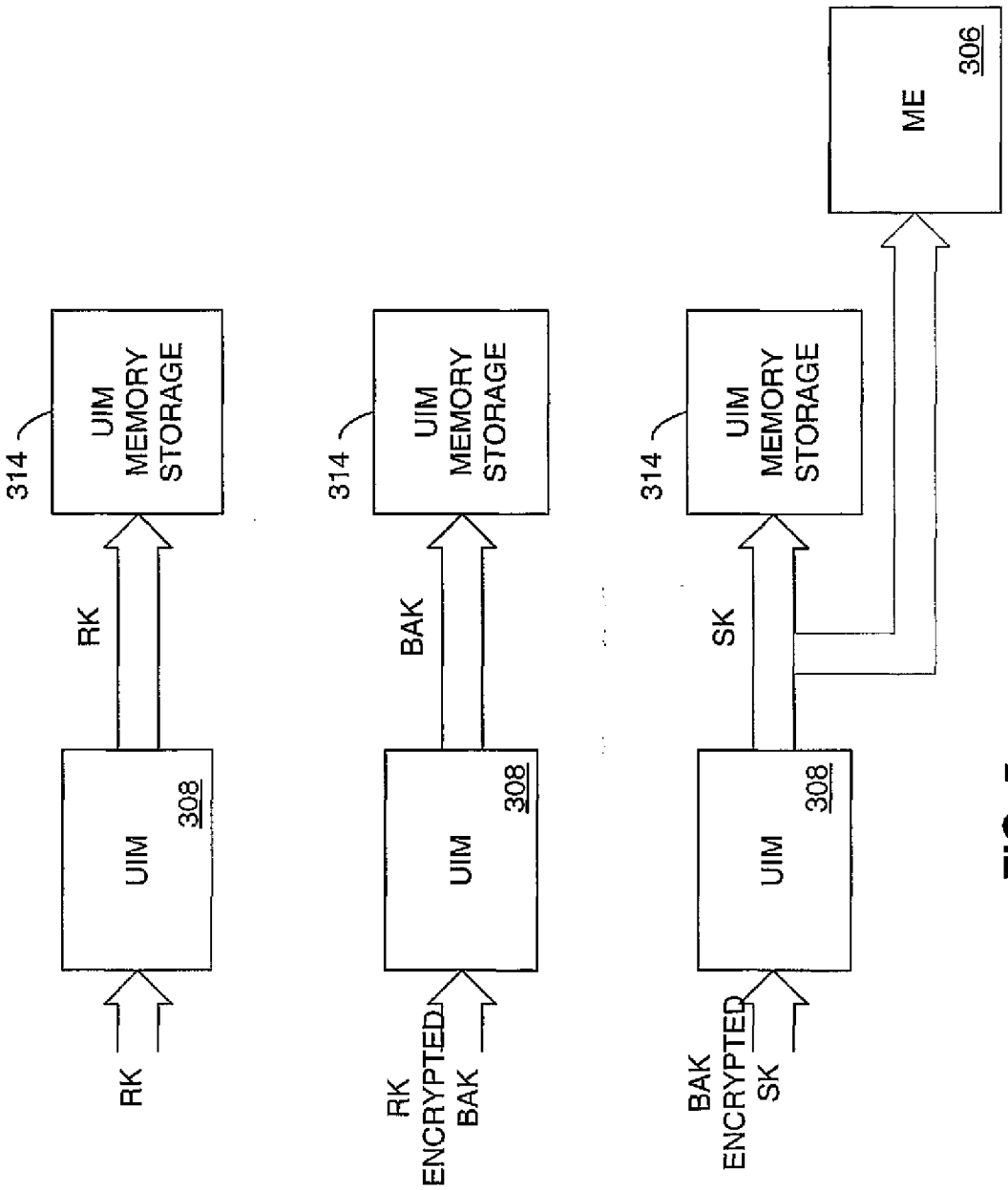

ME
306
UIM
MEMORY
STORAGE
314
UIM
308
RK
BAK
SK
RK
BAK
ENCRYPTED
BAK
SK
ENCRYPTED

FIG. 5

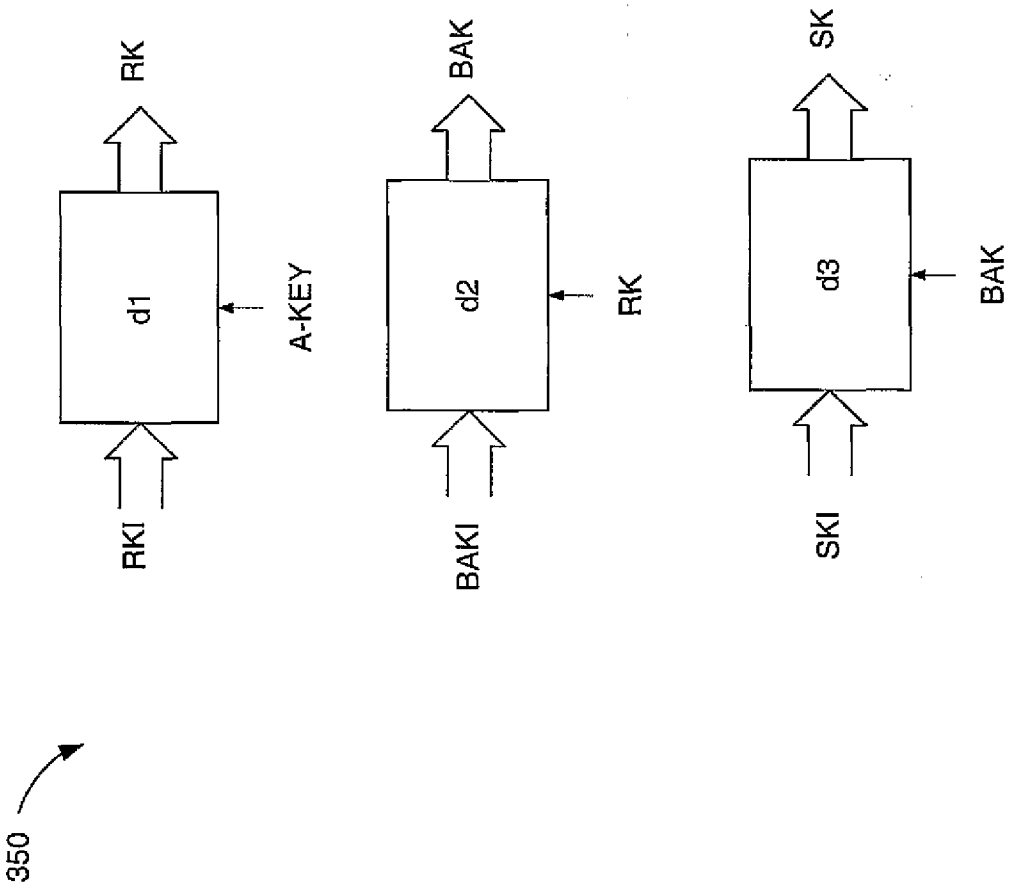


FIG. 6

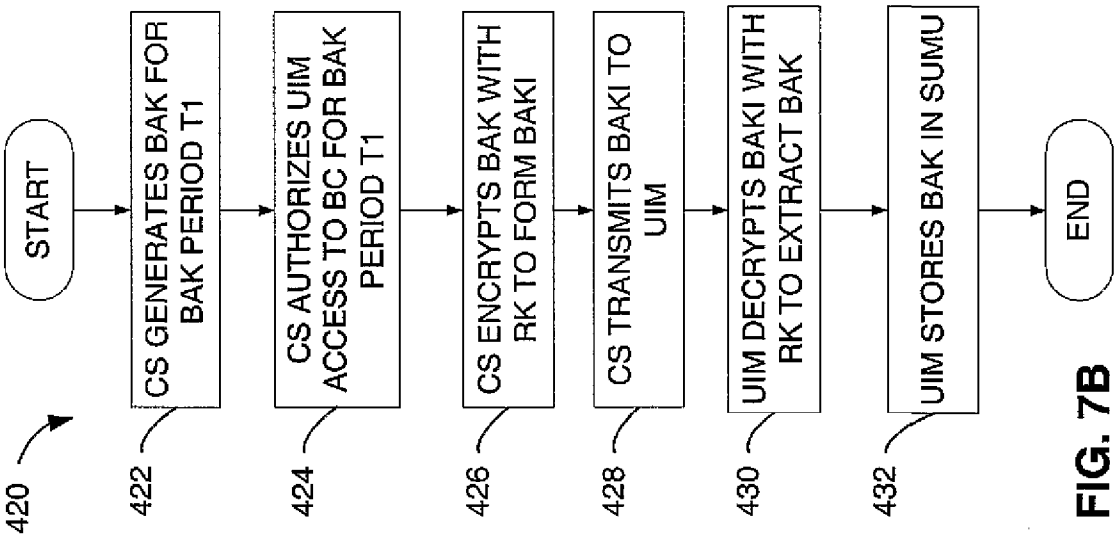

START
CS GENERATES BAK FOR BAK PERIOD T1
CS AUTHORIZES UIM ACCESS TO BC FOR BAK PERIOD T1
CS ENCRYPTS BAK WITH RK TO FORM BAKI
CS TRANSMITS BAKI TO UIM
UIM DECRYPTS BAKI WITH RK TO EXTRACT BAK
UIM STORES BAK IN SUMU
END
420
422
424
426
428
430
432

FIG. 7B

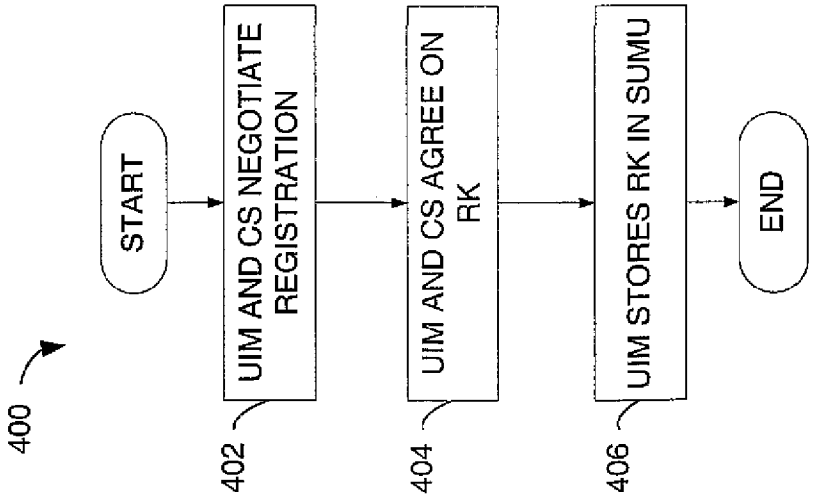

START
UIM AND CS NEGOTIATE REGISTRATION
UIM AND CS AGREE ON RK
UIM STORES RK IN SUMU
END
400
402
404
406

FIG. 7A

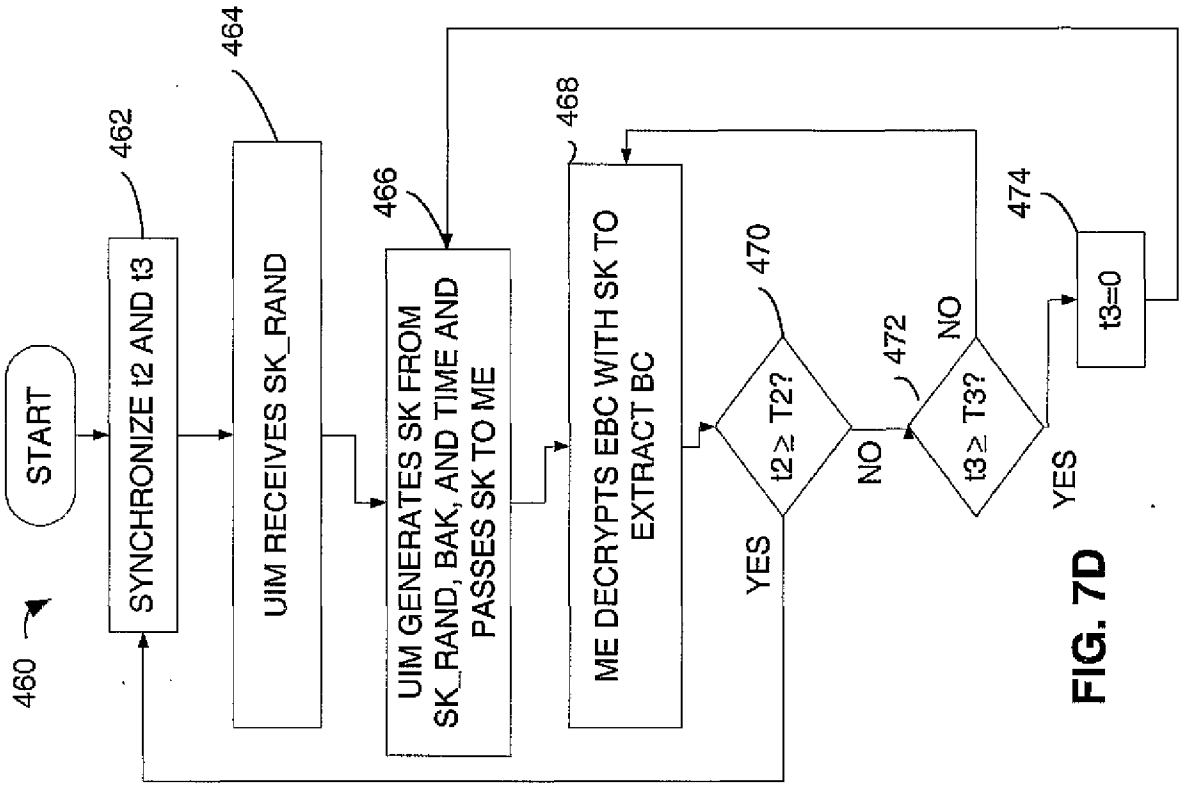

460
START
462
SYNCHRONIZE t2 AND t3
464
UIM RECEIVES SK_RAND
466
UIM GENERATES SK FROM SK_RAND, BAK, AND TIME AND PASSES SK TO ME
468
ME DECRYPTS EBC WITH SK TO EXTRACT BC
470
t2 ≥ T2?
YES
NO
472
t3 ≥ T3?
NO
YES
474
t3=0

FIG. 7D

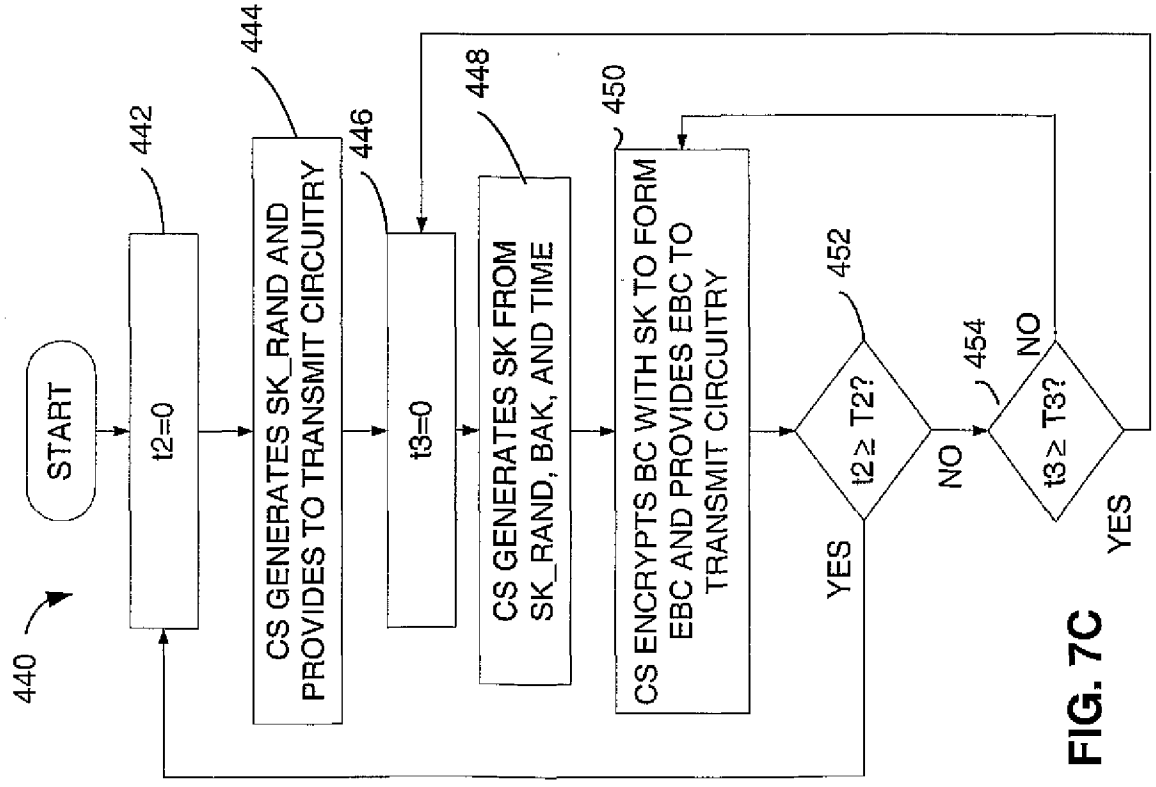

440
START
442
t2=0
444
CS GENERATES SK_RAND AND PROVIDES TO TRANSMIT CIRCUITRY
446
t3=0
448
CS GENERATES SK FROM SK_RAND, BAK, AND TIME
450
CS ENCRYPTS BC WITH SK TO FORM EBC AND PROVIDES EBC TO TRANSMIT CIRCUITRY
452
t2 ≥ T2?
YES
NO
454
t3 ≥ T3?
NO
YES

FIG. 7C

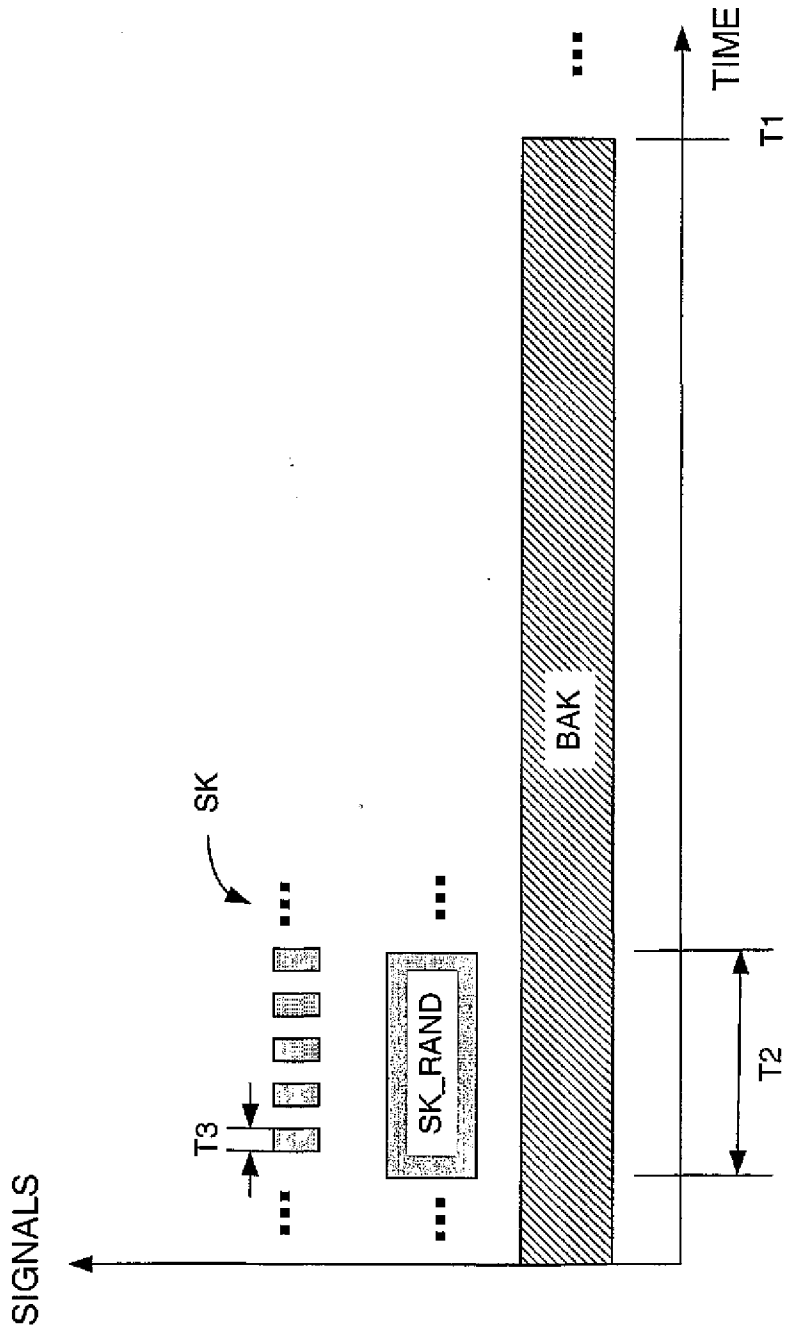


FIG. 7E

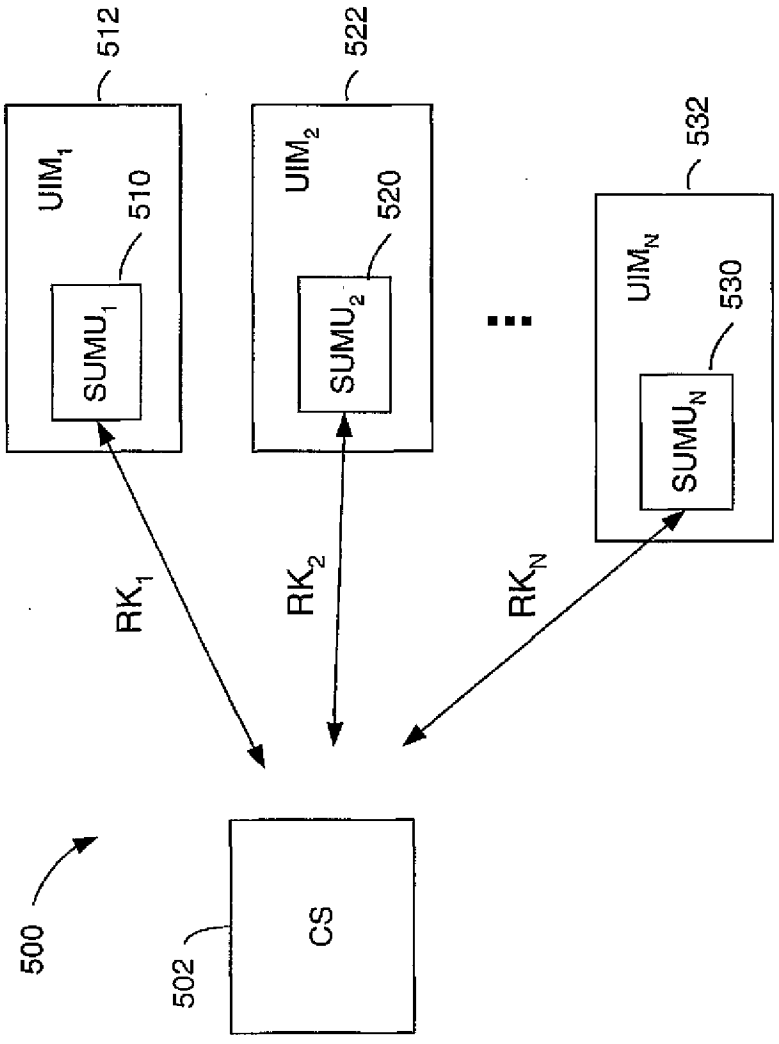

512
522
532
UIM1
510
SUMU1
UIM2
520
SUMU2
UIMN
530
SUMUN
RK1
RK2
RKN
500
502
CS

FIG. 8A

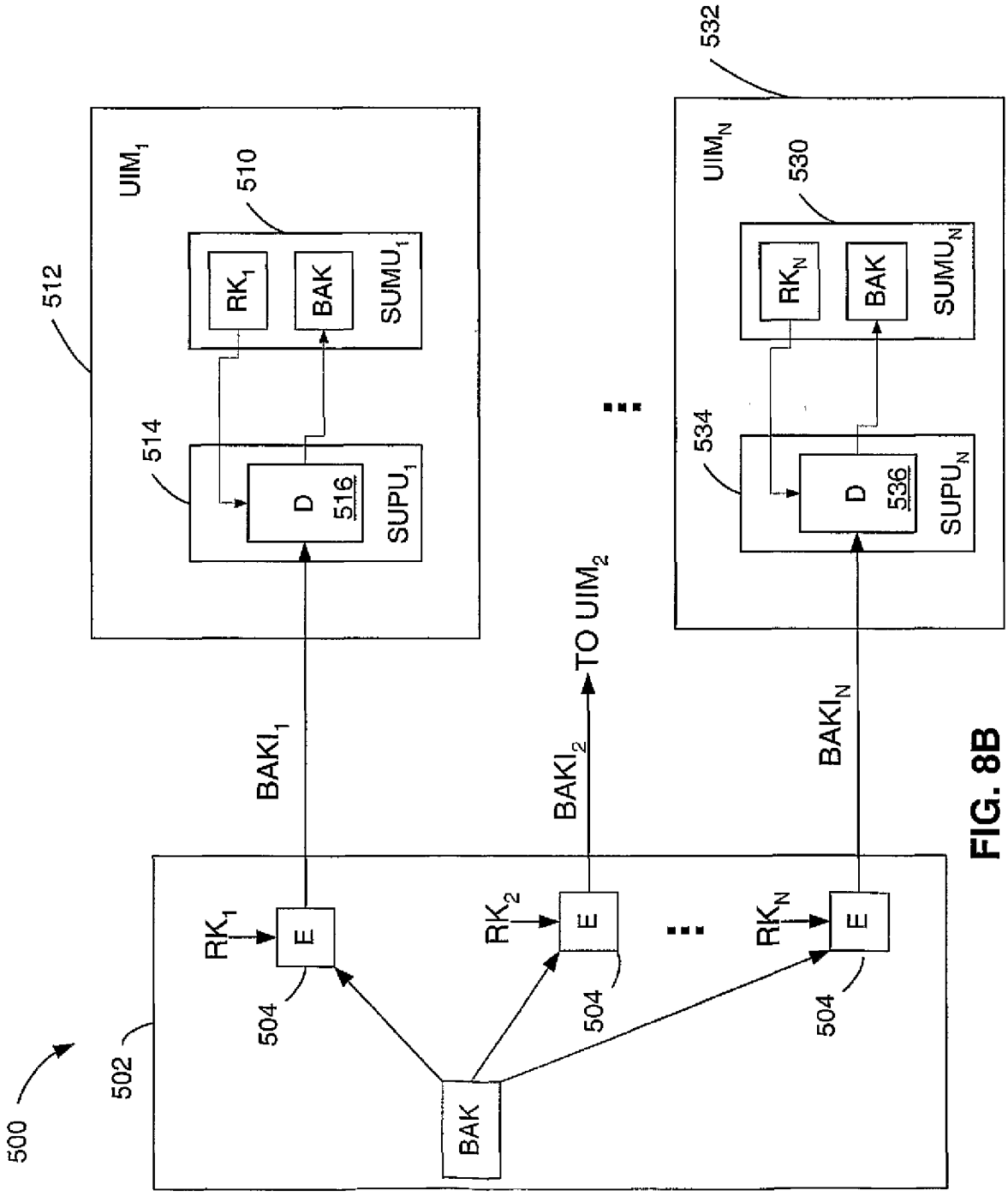

500
502
BAK
504
E
RK_1
RK_2
RK_N
$BAKI_1$
$BAKI_2$
TO UIM_2
$BAKI_N$
512
UIM_1
510
RK_1
BAK
$SUMU_1$
514
D
516
$SUPU_1$
532
UIM_N
530
RK_N
BAK
$SUMU_N$
534
D
536
$SUPU_N$

FIG. 8B

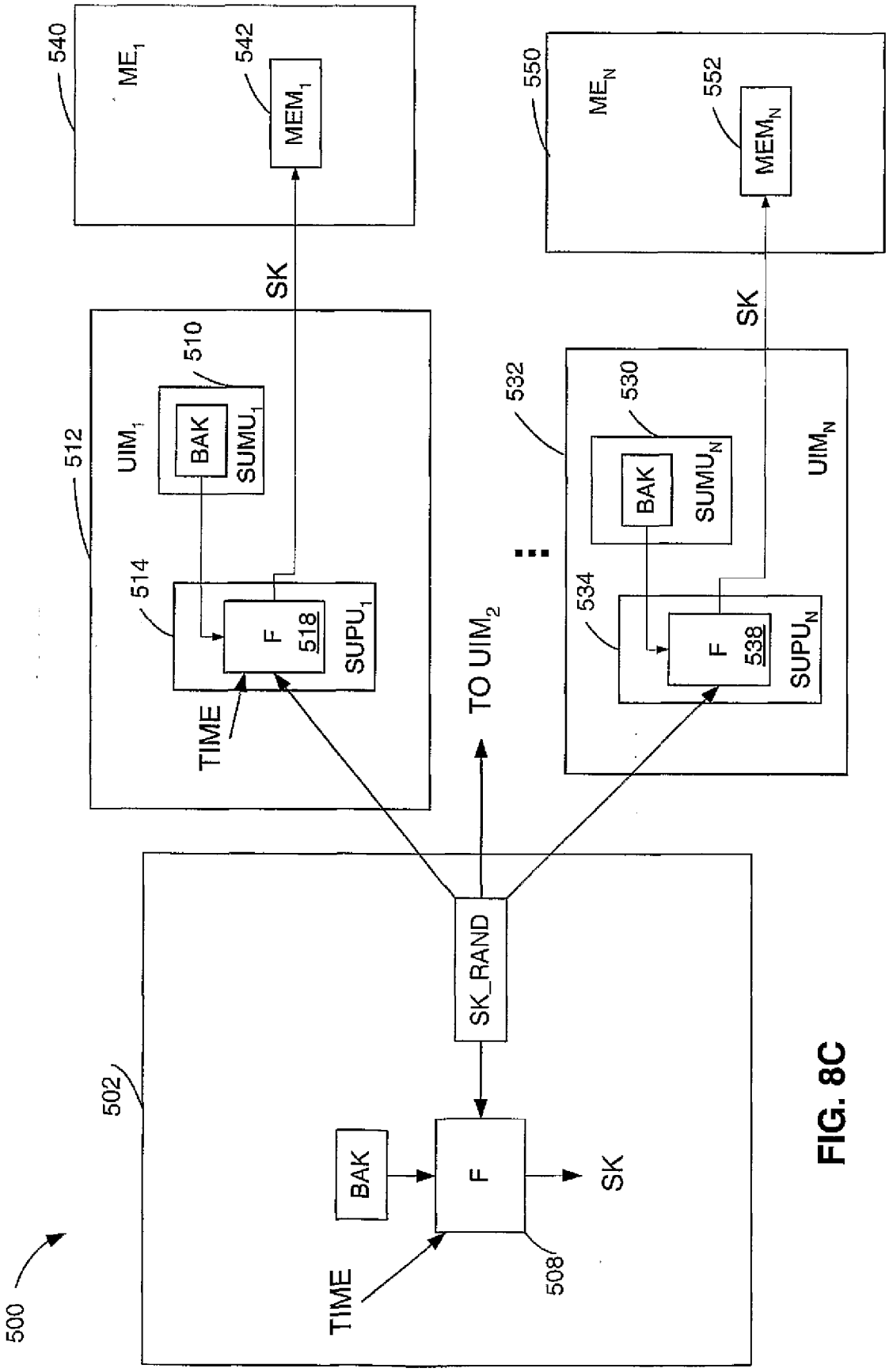

500
502
BAK
F
508
TIME
SK
SK_RAND
TO UIM2
512
UIM1
510
BAK
SUMU1
514
F
518
SUPU1
TIME
SK
540
ME1
542
MEM1
532
UIMN
530
BAK
SUMUN
534
F
538
SUPUN
SK
550
MEN
552
MEMN

FIG. 8C

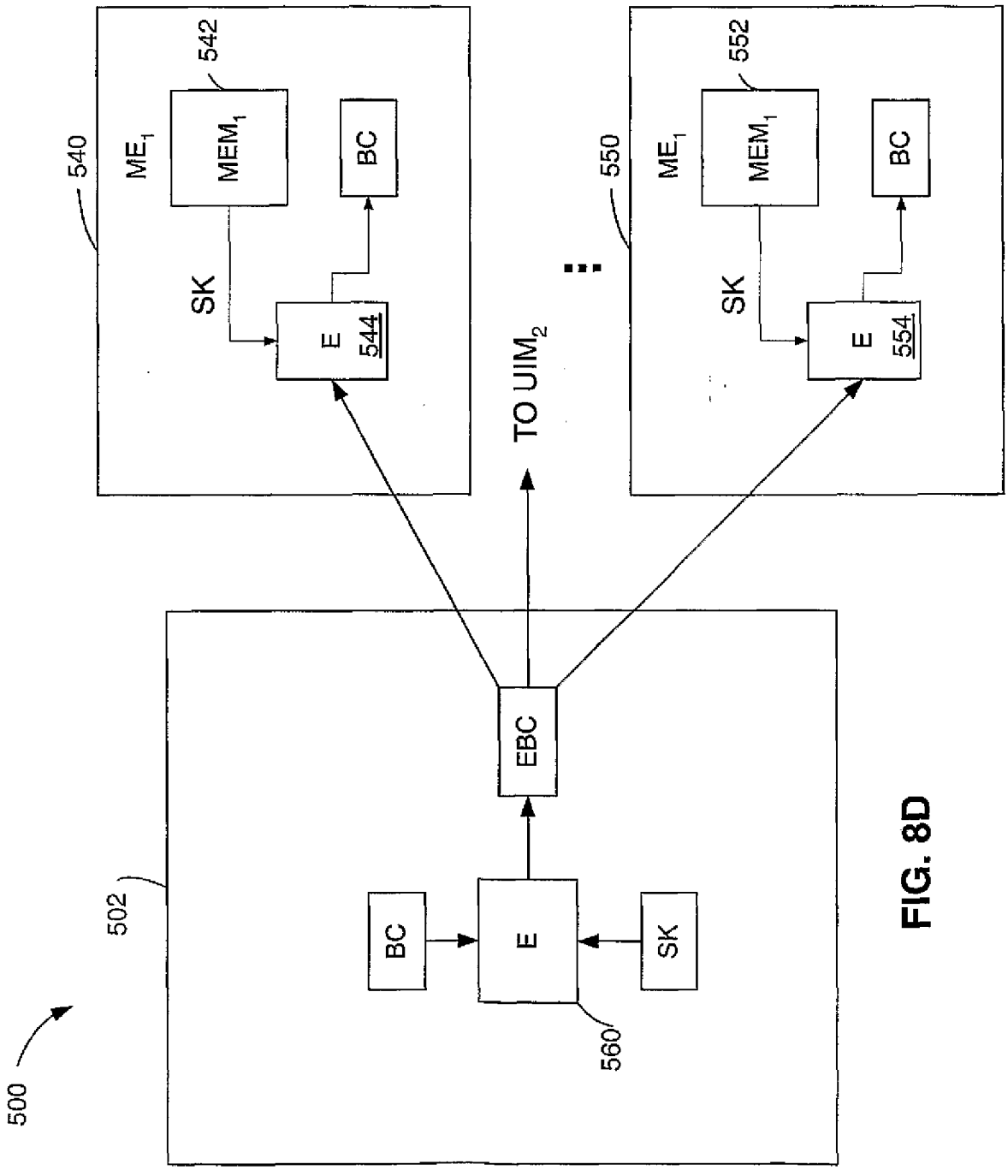

500
502
BC
E
SK
560
EBC
TO UIM2
540
ME1
MEM1
542
BC
SK
E
544
550
ME1
MEM1
552
BC
SK
E
554

FIG. 8D

INTERNATIONAL SEARCH REPORT

PCT/US 02/09835

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MENEZES, OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 551-553,577-581, XP002202082 ISBN: 0-8493-8523-7 page 551 -page 553 page 577 -page 581 ---	1-24
A	BERKOVITS S : "How to Broadcast a Secret" ADVANCES IN CRYPTOLOGY - EUROCRYPT '91 CONFERENCE. SPRINGER-VERLAG, 11 April 1991 (1991-04-11), pages 535-541, XP002202083 Brighton, UK, ISBN: 3-540-54620-0 page 535 -page 536 ---	1-24
	-/--	

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2002	08/07/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	MARCHENT B G ET AL: "Intelligent control of mobile multimedia systems" VEHICULAR TECHNOLOGY CONFERENCE, 1998. VTC 98. 48TH IEEE OTTAWA, ONT., CANADA 18-21 MAY 1998, NEW YORK, NY, USA,IEEE, US, 18 May 1998 (1998-05-18), pages 2047-2051, XP010288261 ISBN: 0-7803-4320-4 the whole document	5,6,21

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 April 2003 (17.04.2003)

PCT

(10) International Publication Number
WO 03/032573 A2

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/US02/32054

(22) International Filing Date: 8 October 2002 (08.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/973,301 9 October 2001 (09.10.2001) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(72) Inventors: HAWKES, Philip; 2/6-8 Belmore Street, Burwood, New South Wales 2134 (AU). LEUNG, Nikolai K., N.; 7710 Takoma Avenue, Takoma Park, MD 20912 (US). ROSE, Gregory G.; 6 Kingston Avenue, Mortlake, New South Wales 2137 (AU).

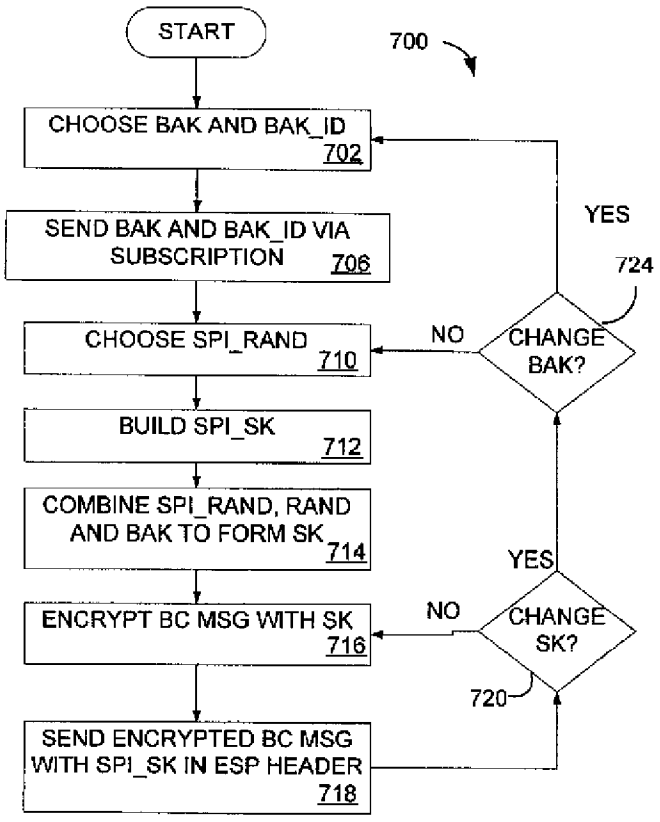
(74) Agents: WADSWORTH, Philip, R. et al.; QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, CA 92121 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM



(57) Abstract: Method and apparatus for secure transmissions. Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user. A short-time updatedkey is encrypted using the broadcast key. The short-time key is available with each broadcast message,wherein sufficient information to calculate the short-time key is provided in an Internet protocol headerpreceding the broadcast content. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.

WO 03/032573 A2

Published:

without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM

BACKGROUND

Field

[1000] The present invention relates to data processing systems generally and specifically, to methods and apparatus for security in a data processing system.

Background

[1001] Security in data processing and information systems, including communications systems, contributes to accountability, fairness, accuracy, confidentiality, operability, as well as a plethora of other desired criteria. Encryption, or the general field of cryptography, is used in electronic commerce, wireless communications, broadcasting, and has an unlimited range of applications. In electronic commerce, encryption is used to prevent fraud in and to verify financial transactions. In data processing systems, encryption is used to verify a participant's identity. Encryption is also used to prevent hacking, protect Web pages, and prevent access to confidential documents, as well as a variety of other security measures.

[1002] Systems employing cryptography, often referred to as cryptosystems, can be partitioned into symmetric cryptosystems and asymmetric cryptosystems. A symmetric encryption system uses a same key (i.e., the secret key) to encrypt and decrypt a message. Whereas an asymmetric encryption system uses a first key (i.e., the public key) to encrypt a message and uses a second, different key (i.e., the private key) to decrypt it. Asymmetric cryptosystems are also called *public key* cryptosystems. A problem exists in symmetric cryptosystems in the secure provision of the secret key from a sender to a recipient. Further, a problem exists when keys or other encryption mechanisms are updated frequently. In a data processing system, methods of securely updating keys incur additional processing time, memory storage and

other processing overhead. In a wireless communication system, updating keys uses valuable bandwidth otherwise available for transmission.

[1003] The prior art does not provide a method for updating keys to a large group of mobile stations in order that they may access an encrypted broadcast. There is a need, therefore, for a secure and efficient method of updating keys in a data processing system. Further, there is a need for a secure and efficient method of updating keys in a wireless communication system.

SUMMARY

[1004] Embodiments disclosed herein address the above stated needs by providing a method for security in a data processing system. In one aspect, a method for secure transmissions includes determining a short term key for a message for transmission, wherein the short term key has a short term key identifier, determining an access key for the message, wherein the access key has an access key identifier, encrypting the message with the access key, forming an Internet protocol header comprising the short term key identifier, and transmitting the encrypted message with the Internet protocol header.

[1005] In another aspect, in a wireless communication system supporting a broadcast service option, an infrastructure element includes a receive circuitry, a user identification unit, operative to recover a short-time key for decrypting a broadcast message, and a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message. The user identification unit including a processing unit operative to decrypt key information. The mobile equipment unit including a memory storage unit for storing a plurality of short term keys and short term key identifiers.

[1006] In still another aspect, a digital signal storage device includes a first set of instructions for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key, a second set of instructions for determining an access key based on the short term key identifier, a third set of instructions for encrypting the short term key identifier with the access key to recover the short term key, and a fourth set of instructions for decrypting the transmission using the short term key.

BRIEF DESCRIPTION OF THE DRAWINGS

[1007] FIG. 1A is a diagram of a cryptosystem.

[1008] FIG. 1B is a diagram of a symmetric cryptosystem.

[1009] FIG. 1C is a diagram of an asymmetric cryptosystem.

[1010] FIG. 1D is a diagram of a PGP encryption system.

[1011] FIG. 1E is a diagram of a PGP decryption system.

[1012] FIG. 2 is a diagram of a spread spectrum communication system that supports a number of users.

[1013] FIG. 3 is a block diagram of the communication system supporting broadcast transmissions.

[1014] FIG. 4 is a block diagram of a mobile station in a wireless communication system.

[1015] FIGs. 5A and 5B illustrate models describing the updating of keys within a mobile station used for controlling broadcast access.

[1016] FIG. 6 is a model describing cryptographic operations within a UIM.

[1017] FIGs. 7A-7D illustrate a method of implementing security encryption in a wireless communication system supporting broadcast transmissions.

[1018] FIG. 7E is a timing diagram of key update periods of a security option in a wireless communication system supporting broadcast transmissions.

[1019] FIGs. 8A-8D illustrate application of a security encryption method in a wireless communication system supporting broadcast transmissions.

[1020] FIG. 9A illustrates the format of an IPSec packet for an Internet Protocol transmission.

[1021] FIG. 9B illustrates a Security Association Identifier or SPI as applicable to an IPSec packet.

[1022] FIG. 9C illustrates a memory storage device for storing SPI information in a mobile station.

[1023] FIG. 9D illustrates a memory storage device for storing Broadcast Access Keys (BAKs) in a mobile station.

[1024] FIGs. 10 and 11 illustrate a method for providing security for a broadcast message in a wireless communication system.

[1025] FIG. 12A illustrates a Security Association Identifier or SPI as applicable to an IPSec packet.

[1026] FIG. 12B illustrates a memory storage device for storing SPI information in a mobile station.

[1027] FIG. 13 and 14 illustrate a method for providing security for a broadcast message in a wireless communication system.

DETAILED DESCRIPTION

[1028] The word "exemplary" is used exclusively herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[1029] Wireless communication systems are widely deployed to provide various types of communication such as voice, data, and so on. These systems may be based on code division multiple access (CDMA), time division multiple access (TDMA), or some other modulation techniques. A CDMA system provides certain advantages over other types of system, including increased system capacity.

[1030] A system may be designed to support one or more standards such as the "TIA/EIA/IS-95-B Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System" referred to herein as the IS-95 standard, the standard offered by a consortium named "3rd Generation Partnership Project" referred to herein as 3GPP, and embodied in a set of documents including Document Nos. 3G TS 25.211, 3G TS 25.212, 3G TS 25.213, and 3G TS 25.214, 3G TS 25.302, referred to herein as the W-CDMA standard, the standard offered by a consortium named "3rd Generation Partnership Project 2" referred to herein as 3GPP2, and TR-45.5 referred to herein as the cdma2000 standard, formerly called IS-2000 MC. The standards cited hereinabove are hereby expressly incorporated herein by reference.

[1031] Each standard specifically defines the processing of data for transmission from base station to mobile, and vice versa. As an exemplary embodiment the following discussion considers a spread-spectrum communication system consistent with cdma2000 systems. Alternate embodiments may incorporate another standard/system. Still other embodiments may apply the security methods disclosed herein to any type of data processing system using a cryptosystem.

[1032] A cryptosystem is a method of disguising messages that allows a specific group of users to extract the message. FIG. 1A illustrates a basic cryptosystem 10. Cryptography is the art of creating and using cryptosystems. Cryptanalysis is the art of breaking cryptosystems, i.e., receiving and understanding the message when you are not within the specific group of users allowed access to the message. The original message is referred to as a plaintext message or plaintext. The encrypted message is called a ciphertext, wherein encryption includes any means to convert plaintext into ciphertext. Decryption includes any means to convert ciphertext into plaintext, i.e., recover the original message. As illustrated in FIG. 1A, the plaintext message is encrypted to form a ciphertext. The ciphertext is then received and decrypted to recover the plaintext. While the terms plaintext and ciphertext generally refer to data, the concepts of encryption may be applied to any digital information, including audio and video data presented in digital form. While the description of the invention provided herein uses the term plaintext and ciphertext consistent with the art of cryptography, these terms do not exclude other forms of digital communications.

[1033] A cryptosystem is based on secrets. A group of entities shares a secret if an entity outside this group cannot obtain the secret without significantly large amount of resources.

[1034] A cryptosystem may be a collection of algorithms, wherein each algorithm is labeled and the labels are called keys. A symmetric encryption system, often referred to as a cryptosystem, uses a same key (i.e., the secret key) to encrypt and decrypt a message. A symmetric encryption system 20 is illustrated in FIG. 1B, wherein both the encryption and decryption utilize a same private key.

[1035] In contrast, an asymmetric encryption system uses a first key (e.g., the public key) to encrypt a message and uses a different key (e.g., the private key) to decrypt it. FIG. 1C illustrates an asymmetric encryption system 30 wherein one key is provided for encryption and a second key for decryption. Asymmetric cryptosystems are also called *public key* cryptosystems. The public key is published and available for encrypting any message, however, only the private key may be used to decrypt the message encrypted with the public key.

[1036] A problem exists in symmetric cryptosystems in the secure provision of the secret key from a sender to a recipient. In one solution, a courier may be used to provide the information, or a more efficient and reliable solution may be to use a public key cryptosystem, such as a public-key cryptosystem defined by Rivest, Shamir, and Adleman (RSA) which is discussed hereinbelow. The RSA system is used in the popular security tool referred to as Pretty Good Privacy (PGP), which is further detailed hereinbelow. For instance, an originally recorded cryptosystem altered letters in a plaintext by shifting each letter by *n* in the alphabet, wherein *n* is a predetermined constant integer value. In such a scheme, an "A" is replaced with a "D," etc., wherein a given encryption scheme may incorporate several different values of *n*. In this encryption scheme "*n*" is the key. Intended recipients are provided the encryption scheme prior to receipt of a ciphertext. In this way, only those knowing the key should be able to decrypt the ciphertext to recover the plaintext. However, by calculating the key with knowledge of encryption, unintended parties may be able to intercept and decrypt the ciphertext, creating a security problem.

[1037] More complicated and sophisticated cryptosystems employ strategic keys that deter interception and decryption from unintended parties. A classic cryptosystem employs encryption functions *E* and decryption functions *D* such that:

$$D\_K(E\_K(P)) = P, \text{ for any plaintext } P. \qquad (1)$$

[1038] In a public-key cryptosystem, E_K is easily computed from a known ``public key'' *Y* which in turn is computed from *K*. The public key *Y* is published, so that anyone can encrypt messages. The decryption function D_K is computed from public key *Y*, but only with knowledge of a private key *K*. Without the private key *K* an unintended recipient may not decrypt the ciphertext

so generated. In this way only the recipient who generated *K* can decrypt messages.

[1039] RSA is a public-key cryptosystem defined by Rivest, Shamir, and Adleman, wherein, for example, plaintexts consider positive integers up to 2^{512}. Keys are quadruples (*p,q,e,d*), with *p* given as a 256-bit prime number, *q* as a 258-bit prime number, and *d* and *e* large numbers with (*de* - 1) divisible by (*p*-1)(*q*-1). Further, define the encryption function as:

$$E\_K(P) = P^e \bmod pq,\ D\_K(C) = C^d \bmod pq. \qquad (2)$$

[1040] While, E_K is easily computed from the pair (*pq,e*), there is no known simple way to compute D_K from the pair (*pq,e*). Therefore, the recipient that generates K can publish (*pq,e*). It is possible to send a secret message to the recipient as he is the one able to read the message.

[1041] PGP combines features from symmetric and asymmetric encryption. FIGs. 1D and 1E illustrate a PGP cryptosystem 50, wherein a plaintext message is encrypted and recovered. In FIG. 1D, the plaintext message is compressed to save modem transmission time and disk space. Compression strengthens cryptographic security by adding another level of translation to the encrypting and decrypting processing. Most cryptanalysis techniques exploit patterns found in the plaintext to crack the cipher. Compression reduces these patterns in the plaintext, thereby enhancing resistance to cryptanalysis. Note that one embodiment does not compress: plaintext, or other messages that are too short to compress, or which don't compress well.

[1042] PGP then creates a *session key,* which is a one-time-only secret key. This key is a random number that may be generated from any random event(s), such as random movements of a computer mouse and/or the keystrokes while typing. The session key works with a secure encryption algorithm to encrypt the plaintext, resulting in ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. The public key-encrypted session key is transmitted along with the ciphertext to the recipient.

[1043] For decryption, as illustrated in FIG. 1E, the recipient's copy of PGP uses a private key to recover the temporary session key, which PGP then uses to decrypt the conventionally encrypted ciphertext. The combination of encryption methods takes advantage of the convenience of public key

encryption and the speed of symmetric encryption. Symmetric encryption is generally much faster than public key encryption. Public key encryption in turn provides a solution to key distribution and data transmission issues. In combination, performance and key distribution are improved without any sacrifice in security.

[1044] A key is a value that works with a cryptographic algorithm to produce a specific ciphertext. Keys are basically very large numbers. Key size is measured in bits. In public key cryptography, security increases with key size, however, public key size and the symmetric encryption private key size are not generally related. While the public and private keys are mathematically related, a difficulty arises in deriving a private key given only a public key. Deriving the private key is possible given enough time and computing power, making the selection of key size an important security issue. The optimal goal is to maximize the size of the key for security concerns, while minimizing key size to facilitate quick processing. Larger keys will be cryptographically secure for a longer period of time. An additional consideration is the expected interceptor, specifically: 1) what is the importance of a message to a third party; and 2) how much resource will a third party have to decrypt the message.

[1045] Note that keys are stored in encrypted form. PGP specifically stores keys in two files: one for public keys and one for private keys. These files are called *keyrings*. In application, a PGP encryption system adds the public keys of target recipients to the sender's public keyring. The sender's private keys are stored on the sender's private keyring.

[1046] As discussed in the examples given hereinabove, the method of distributing the keys used for encryption and decryption can be complicated. The ``key exchange problem'' involves first ensuring that keys are exchanged such that both the sender and receiver can perform encryption and decryption, respectively, and for bi-directional communication, such that the sender and receiver can both encrypt and decrypt messages. Further, it is desired that key exchange be performed so as to preclude interception by a third and unintended party.

[1047] Finally, an additional consideration is authentication, providing assurance to the receiver that a message was encrypted by an intended sender

and not a third party. In a private key exchange system, the keys are exchanged secretly providing improved security upon successful key exchange and valid authentication. Note that the private key encryption scheme implicitly provides authentication. The underlying assumption in a private key cryptosystem is that only the intended sender will have the key capable of encrypting messages delivered to the intended receiver. While public-key cryptographic methods solve a critical aspect of the `key-exchange problem', specifically their resistance to analysis even with the presence a passive eavesdropper during exchange of keys, still, they do not solve all problems associated with key exchange. In particular, since the keys are considered `public knowledge' (particularly with RSA), some other mechanism is desired to provide authentication. Authentication is desired as possession of keys alone, while sufficient to encrypt messages, is no evidence of a particular unique identity of the sender, nor is possession of a corresponding decryption key by itself sufficient to establish the identity of the recipient.

[1048] One solution is to develop a key distribution mechanism that assures that listed keys are actually those of the given entities, sometimes called a trusted authority, certificate authority, or third part escrow agent. The authority typically does not actually generate keys, but does ensure that the lists of keys and associated identities kept and advertised for reference by senders and receivers are correct and not compromised. Another method relies on users to distribute and track each other's keys and trust in an informal, distributed fashion. Under RSA, if a user wishes to send evidence of their identity in addition to an encrypted message, a signature is encrypted with the private key. The receiver can use the RSA algorithm in reverse to verify that the information decrypts, such that only the sender could have encrypted the plaintext by use of the secret key. Typically the encrypted `signature' is a `message digest' that comprises a unique mathematical `summary' of the secret message (if the signature were static across multiple messages, once known previous receivers could use it falsely). In this way, theoretically, only the sender of the message could generate a valid signature for that message, thereby authenticating it for the receiver.

[1049] A message digest is often computed using a cryptographic hash function. A cryptographic hash function computes a value (with a fixed number of bits) from any input, regardless of the length of the input. One property of a cryptographic hash function is this: given an output value, it is computationally difficult to determine an input that will result in that output. An example of a cryptographic hash function is SHA-1 as described in "Secure Hash Standard," FIPS PUB 180-1, promulgated by the Federal Information Processing Standards Publications (FIPS PUBS) and issued by the National Institute of Standards and Technology.

[1050] FIG. 2 serves as an example of a communications system 100 that supports a number of users and is capable of implementing at least some aspects and embodiments of the invention. Any of a variety of algorithms and methods may be used to schedule transmissions in system 100. System 100 provides communication for a number of cells 102A through 102G, each of which is serviced by a corresponding base station 104A through 104G, respectively. In the exemplary embodiment, some of base stations 104 have multiple receive antennas and others have only one receive antenna. Similarly, some of base stations 104 have multiple transmit antennas, and others have single transmit antennas. There are no restrictions on the combinations of transmit antennas and receive antennas. Therefore, it is possible for a base station 104 to have multiple transmit antennas and a single receive antenna, or to have multiple receive antennas and a single transmit antenna, or to have both single or multiple transmit and receive antennas.

[1051] Terminals 106 in the coverage area may be fixed (i.e., stationary) or mobile. As shown in FIG. 2, various terminals 106 are dispersed throughout the system. Each terminal 106 communicates with at least one and possibly more base stations 104 on the downlink and uplink at any given moment depending on, for example, whether soft handoff is employed or whether the terminal is designed and operated to (concurrently or sequentially) receive multiple transmissions from multiple base stations. Soft handoff in CDMA communications systems is well known in the art and is described in detail in U.S. Patent No. 5,101,501, entitled "Method and system for providing a Soft

Handoff in a CDMA Cellular Telephone System", which is assigned to the assignee of the present invention.

[1052] The downlink refers to transmission from the base station to the terminal, and the uplink refers to transmission from the terminal to the base station. In the exemplary embodiment, some of terminals 106 have multiple receive antennas and others have only one receive antenna. In FIG. 2, base station 104A transmits data to terminals 106A and 106J on the downlink, base station 104B transmits data to terminals 106B and 106J, base station 104C transmits data to terminal 106C, and so on.

[1053] Increasing demand for wireless data transmission and the expansion of services available via wireless communication technology have led to the development of specific data services. One such service is referred to as High Data Rate (HDR). An exemplary HDR service is proposed in "EIA/TIA-IS856 cdma2000 High Rate Packet Data Air Interface Specification" referred to as "the HDR specification." HDR service is generally an overlay to a voice communication system that provides an efficient method of transmitting packets of data in a wireless communication system. As the amount of data transmitted and the number of transmissions increases, the limited bandwidth available for radio transmissions becomes a critical resource. There is a need, therefore, for an efficient and fair method of scheduling transmissions in a communication system that optimizes use of available bandwidth. In the exemplary embodiment, system 100 illustrated in FIG. 2 is consistent with a CDMA type system having HDR service.

[1054] According to one embodiment, the system 100 supports a high-speed multimedia broadcasting service referred to as High-Speed Broadcast Service (HSBS). An example application for HSBS is video streaming of movies, sports events, etc. The HSBS service is a packet data service based on the Internet Protocol (IP). According to the exemplary embodiment, a service provider indicates the availability of such high-speed broadcast service to the users. The users desiring the HSBS service subscribe to receive the service and may discover the broadcast service schedule through advertisements, Short Management System (SMS), Wireless Application Protocol (WAP), etc. Mobile users are referred to as Mobile Stations (MSs). Base Stations (BSs) transmit

HSBS related parameters in overhead messages. When an MS desires to receive the broadcast session, the MS reads the overhead messages and learns the appropriate configurations. The MS then tunes to the frequency containing the HSBS channel, and receives the broadcast service content.

[1055] The service being considered is a high-speed multimedia broadcasting service. This service is referred to as High-Speed Broadcast Service (HSBS) in this document. One such example is video streaming of movies, sports events, etc. This service will likely be a packet data service based on the Internet Protocol (IP).

[1056] The service provider will indicate the availability of such high-speed broadcast service to the users. The mobile station users who desire such service will subscribe to receive this service and may discover the broadcast service schedule through advertisements, SMS, WAP, etc. Base stations will transmit broadcast service related parameters in overhead messages. The mobiles that wish to listen to the broadcast session will read these messages to determine the appropriate configurations, tune to the frequency containing the high-speed broadcast channel, and start receiving the broadcast service content.

[1057] There are several possible subscription/revenue models for HSBS service, including free access, controlled access, and partially controlled access. For free access, no subscription is needed by the mobiles to receive the service. The BS broadcasts the content without encryption and interested mobiles can receive the content. The revenue for the service provider can be generated through advertisements that may also be transmitted in the broadcast channel. For example, upcoming movie-clips can be transmitted for which the studios will pay the service provider.

[1058] For controlled access, the MS users subscribe to the service and pay the corresponding fee to receive the broadcast service. Users that are not subscribed to the service are not able to receive the HSBS service. Controlled access can be achieved by encrypting the HSBS transmission/content so that only the subscribed users can decrypt the content. This may use over-the-air encryption key exchange procedures. This scheme provides strong security and prevents theft-of-service.